DISEÑO DEL PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR

NORBERTO CASTAÑO URBINA
CRISTIAN FUENTES CASTILLO

CORPORACIÓN UNIVERSITARIA DE LA COSTA – CUC
FACULTAD DE CONTADURÍA PÚBLICA
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARANQUILLA
2012

DISEÑO DEL PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR

NORBERTO CASTAÑO URBINA
CRISTIAN FUENTES CASTILLO

TRABAJO DE TESIS PARA OPTAR EL TITULO DE ESPECIALISTA EN AUDITORIA DE SISTEMAS DE INFORMACION

VÍCTOR MONTAÑO ARDILLA
ASESOR

CORPORACIÓN UNIVERSITARIA DE LA COSTA – CUC
FACULTAD DE CONTADURIA PÚBLICA
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARANQUILLA
2012

NOTA DE ACEPTACIÓN:

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

A Dios por darme la oportunidad de vivir y las bendiciones recibidas.
A mi esposa por su comprensión y tolerancia.
A mi hijo por sacrificar su tiempo de disfrute con migo.
A mis padres por su apoyo incondicional
Al cuerpo de docentes por todos los conocimientos impartidos.
A mi tutor por la comprensión, dedicación motivación y apoyo constantes.

NORBERTO CASTAÑO URBINA

A Dios por todas las bendiciones recibidas.
A mis padres por su apoyo su esfuerzo y apoyo incondicional
Al cuerpo de docentes por todos los conocimientos impartidos.
A mi tutor la comprensión, dedicación motivación y apoyo constantes.

CRISTIAN RAUL FUENTES CASTILLO

AGRADECIMIENTO

A Dios Todopoderoso, por permitirnos alcanzar esta meta.

A la Corporación Universitaria de la Costa, que me impulsó a realizar este Proyecto.

A todas aquellas personas que de una u otra manera nos apoyaron durante el desarrollo del presente proyecto. VÍCTOR MANUEL MONTAÑO ARDILA, ROBERTO CARLOS DIAZ, HEYNER AROCA. JHONY FLORES, OLGA HERNANDEZ

NORBERTO URBINA CASTAÑO

CRISTIAN RAUL FUENTES CASTILLO

CONTENIDO

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

El presente proyecto se denomina DISEÑO DEL PLAN ESTRATÉGICO DE TECNOLOGÍA INFORMÁTICA Y MODELO DE GESTIÓN DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LÓPEZ – VALLEDUPAR fue realizado conceptualmente en cuatro estándares para la construcción de un modelo de Gobierno de TI y que gozan de gran aceptación mundial, por lo que han sido denominados como “Mejores Prácticas”.

El Modelo Cobit, las normas ISO 27001, 27002, 20000 e ITIL representan las mejores prácticas, para su implementación en las organizaciones y la articulación de cada una de ellas conforman un modelo guía útil para una adecuada planificación de TI, para las entidades de salud como la ESE HOSPITAL ROSARIO PUMAREJO DE LÓPEZ – VALLEDUPAR brindara una oportunidad de alinear las estrategias de TI con las estrategias del hospital, de alcanzar el uso optimo de todos sus recursos que ayudaran a satisfacer las necesidades de la entidad y los requisitos de los usuarios, Cumplir con la legislación, prestar un mejor servicio, revisarse y mejorarse de forma continua. Con la implementación de estos estándares contribuirá a proporcionar una base de control de TI en las entidades de salud.

INTRODUCCIÓN

El presente proyecto tomará como base el Plan de Gestión Institucional (PGI) o Plan Estratégico Corporativo (PEC) y construirá un Plan Estratégico de Tecnología Informática (PETI) que permita apoyar de forma efectiva y eficiente los objetivos corporativos. De igual manera realizará un análisis de los procedimientos establecidos en el Área de Tecnología Informática para la atención de requerimientos de usuarios, manejo de incidentes y problemas, gestión del cambio y otros aspectos que requieren ser normalizados para optimizar la gestión de servicios del área.

Actualmente la ESE (Empresa Social del Estado) Hospital Rosario Pumarejo de López de la ciudad de Valledupar no cuenta con un plan estratégico de TI y tampoco con un modelo estructurado para la gestión de servicios de TI, por ello la planeación se construye anualmente respondiendo a solicitudes puntuales y priorizadas por el criterio subjetivo del Jefe de Sistemas.

El Departamento de Sistemas cuenta con dos ingenieros provistos por una empresa contratista y dos estudiantes en práctica ocasionales. Cada uno de ellos atiende las solicitudes de usuario en la medida de sus capacidades o la escalan para ser atendidas por el Jefe de Sistemas. No se está llevando registro de incidentes y problemas como tampoco de las acciones realizadas y el tiempo requerido para su solución.

El proyecto se fundamentará conceptualmente en cuatro estándares para la construcción de un modelo de Gobierno de TI y que gozan de gran aceptación mundial, por lo que han sido denominados como “Mejores Prácticas”, estos son:

a. COBIT4.1.: Marco de referencia para el Gobierno de TI.
b. Norma ISO 27001 e ISO 27002. : Sistema de Gestión de la Seguridad de la Información.
c. Norma ISO 20000.: Estandard para certificar la Gestión de Servicios de TI de las Empresas y Organizaciones.
d. ITIL: Estándar para la Gestión de Servicios de TI.

1. PLANTEAMIENTO DEL PROBLEMA

La tecnología informática se erige como uno de los principales factores críticos del éxito de las organizaciones. Su aplicabilidad es cada vez mayor y las organizaciones dependen crecientemente de ella para la toma oportuna y confiable de sus decisiones; no obstante, el crecimiento informático en la mayoría de las empresas se realiza de forma no programada, es decir, no existe una planeación estratégica que determine la ruta tecnológica y el plan de inversiones. Las decisiones se toman de forma subjetiva cobijadas por planes que se trazan con extensión de un año.

Por otro lado los procedimientos para la gestión de servicios de TI se encuentran en su mayoría indocumentados lo que los torna informales y poco eficientes en su atención y solución. Adicionalmente, como no existe un proceso de evaluación y priorización se genera una excesiva pérdida de tiempo por parte del Jefe de Sistemas.

La creación de estándares para la definición de estructuras administrativas que redunden en una eficiente y efectiva gestión de servicios es preocupación de asociaciones internacionales de profesionales, quienes ya han sido aplicados exitosamente a nivel mundial lo que les ha permitido ser catalogados dentro de las mejores prácticas.

Entidades del sector oficial en Colombia han desarrollado planes encaminados a construir un adecuado Modelo de Gobierno de TI con reconocido éxito. En el sector salud no se conoce aún ningún avance en este sentido, pero el proyecto a desarrollar en la ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ sentará las bases para ello.

Bajo la anterior perspectiva se plantea como interrogantes en la presente investigación, los siguientes:

¿Cómo optimizar la ejecución del plan estratégico corporativo en la ESE HOSPITAL PUMAREJO DE LOPEZ a partir del diseño de un adecuado plan estratégico de tecnología informática y la definición de un Sistema de Gestión de Servicios de TI ajustado a sus necesidades?

- ¿Porque realizar un diagnostico de TI de la ESE Hospital Rosario Pumarejo de López a través de los modelos de Madures. (CMMI)?
- ¿Cuáles son los objetivos del Plan de Gestión Institucional (PGI) o Plan Estratégico Corporativo (PEC) que requieran apoyo de Tecnología Informática?
- ¿Cuál es el Plan Estratégico de Tecnología Informática (PETI) alineado con el PEC?
- ¿Qué servicios de TI ofrece el Área de Informática?
- ¿Qué nuevos servicios derivados de la implantación del PETI?
- ¿Cuál es la estructura organizativa y procedimientos para la óptima Gestión de Servicios de TI?

2. JUSTIFICACIÓN E IMPORTANCIA DEL PROYECTO

El contexto de esta investigación apunta al estudio concienzudo del impacto que las Tecnologías de Información tienen en el mundo empresarial hoy como factor diferenciador de las empresas, con base lo anterior un elemento clave para el aseguramiento del éxito y un manejo eficiente de las entidades de salud, es la administración adecuada de la información y de las Tecnologías de información y comunicación, desde la planeación y organización, en vista que existen entidades de salud que no han determinado un marco de trabajo para auditorias integrales de sistemas que ayuden a gestionar estas tecnologías, se hace necesario recurrir a buenas practicas generalmente aplicables y aceptables para medir en forma comparativa tanto su ambiente de TI existente, como su ambiente planeado.

Los estándares COBIT4.1 (Marco de referencia para el Gobierno de TI.), Norma ISO 27001 e ISO 27002 (Sistema de Gestión de la Seguridad de la Información), Norma ISO 20000 (Estandard para certificar la Gestión de Servicios de TI de las Empresas y Organizaciones), ITIL (Estándar para la Gestión de Servicios de TI) permiten disminuir la brecha existente entre los requerimientos de control, los aspectos técnicos y el riesgo del **HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR** orientado siempre a la Tecnología de la información como los clientes, Proveedores, Personal, Control Interno y externo, Evaluación de los sistemas administrativos contables, hardware, software.

En el entorno empresarial moderno no se duda en un instante en acudir a estándares, normas técnicas, regulación y mejores prácticas para encontrar soluciones estratégicas a la pregunta básica de cómo gestionar una organización, en especial y en nuestro caso particular, desde lo tecnológico. Para las entidades de salud esto se logra empezando a aplicar buenas practicas como ITIL, COBIT, ISO 2700X e ISO 9000, así

como procedimientos de Administración de Riesgos, con el fin de tener en cuenta como aspectos esenciales el Gobierno de TI, la Gestión del Servicio, Seguridad de la Información y Teoría de Riesgos, en concordancia con los tres grandes tópicos que exige la auditoría de hoy y a nivel de cascada: Gobierno, Riesgos, Control.

De ahí que la investigación acometida pretenda dilucidar un camino factible en la consecución de un PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR en pro de elaborar un plan y un modelo, que ofrezcan una solución económica, oportuna y beneficiosa para la realización de auditorías en las entidades de salud.

3. OBJETIVOS DEL PROYECTO

3.1 Objetivo General del Proyecto

Diseñar un Plan Estratégico de tecnología informática y la definición de un Sistema de Gestión de Servicios de TI ajustado a las necesidades de la ESE HOSPITAL PUMAREJO DE LOPEZ.

3.2 Objetivos Específicos del Proyecto

- Realizar un diagnostico de TI de la ESE Hospital Rosario Pumarejo de López a través de los modelos de Madures. (CMMI).
- Identificar los objetivos del Plan de Gestión Institucional (PGI) o Plan Estratégico Corporativo (PEC) que requieran apoyo de Tecnología Informática.
- Diseñar un Plan Estratégico de Tecnología Informática (PETI) alineado con el PEC.
- Identificar los servicios de TI actualmente ofrecidos por el Área de Informática.
- Definir nuevos servicios derivados de la implantación del PETI.
- Establecer estructura organizativa y procedimientos para la óptima Gestión de Servicios de TI.

4. DELIMITACION

4.1 Delimitación Especial

Esta investigación tendrá como marco de acción el **HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR,** que es una Empresa Social del Estado.

Para efectos del proyecto, se tendrá como referencia la evolución tecnológica que ha tenido el hospital, además el trabajo que ha realizado actualmente el hospital, con relación a la infraestructura tecnológica, ya que se hará un análisis y articulación entre los estándares COBIT, ITIL y normas técnicas ISO 27002.

5. MARCO TEÓRICO Y ESTADO DEL ARTE

La búsqueda de la calidad a través de una metodología científica, esta dirigida a que todo prestador de servicio se involucre en el proceso de mejoramiento continúo en busca de la satisfacción del usuario mediante un proceso de excelencia.

La promoción de la calidad ha propiciado toda una generación de cambios en las distintas organizaciones, convirtiendo a las instituciones en entes capaces de liderar su propio destino, pero sobre todo, busca desarrollar motivaciones para llenar las expectativas del siglo XXI.

Con la puesta en marcha de la Ley 100 de 1993 y sus decretos reglamentarios, el concepto de calidad se ha convertido en una constante para quien brinda el servicio de salud. No ajenos a esta premisa, la empresa social del estado Hospital Rosario Pumarejo de López presenta a ustedes el portafolio de servicios que manifiesta que estamos, Creciendo Para Todos con Calidad! Basados en la concepción de garantizar a los usuarios del servicio de salud, el mayor beneficio a un costo razonable y eficiente, nos apropiamos de nuestro objeto social y de una plataforma estratégica que permite hacer de la E.S.E., la mejor opción de prestación de servicios de salud de segundo nivel de atención en el departamento.

En la década de los 30 siendo presidente de la República de Colombia el doctor Alfonso López Pumarejo, se ordenó la construcción del Hospital Rosario Pumarejo de López en el municipio de Valledupar, en unos terrenos ubicados en el barrio Hernando de Santana en un área de 7.769 m2, mediante la ley 28 de 1936 reglamentada por el Dec. Ejecutivo Nº 1636 de 1942.

Su infraestructura fue terminada en 1942, ya concluida la construcción, este fue bautizado con el nombre de Rosario Pumarejo de López en honor a la matrona Vallenata, madre del presidente Alfonso López Pumarejo. En 1942 Colombia se encuentra en conflicto bélico con la república de Venezuela, de forma estratégica las instalaciones del hospital fueron ocupadas por el batallón Bomboná como base militar hasta el año 1949. Esto genera un movimiento de tipo local logrando la recuperación del hospital y posteriormente en el año de 1950, el doctor José Antonio Socarras asume el cargo como primer director científico, en asocio con una junta de salud conformada por: un representante de la Curia, uno del cuerpo médico, el director de una entidad crediticia, un representante del gobierno nacional y un representante de la comunidad.

El 10 de Diciembre de 1994, el Hospital Rosario Pumarejo de López fue elevado a la categoría de Entidad Pública prestadora de servicios de salud, como Empresa Social del Estado, E.S.E., por mandato de la ordenanza Nº 048 promulgada por la Asamblea del Departamento del Cesar, el 6 de Diciembre de 1995, adquirió su personería jurídica que lo clasifica como Hospital de Segundo Nivel de Atención. El 26 de Diciembre de 1999 se firma el convenio de desempeño y el de eficiencia entre el Hospital y los Ministerios de Desarrollo y Salud y el Departamento del Cesar, el Convenio de Desempeño 424/99, suscrito entre el Ministerio de Salud, el Departamento del Cesar y el Hospital, fija unas metas de cumplimiento a cinco años, evaluables de acuerdo con lo establecido en el Comité Técnico Territorial, convenio que se ha constituido en el norte del Hospital.

Prestar servicios de salud de segundo nivel de atención en concordancia con nuestra capacidad tecnológica y científica. Complementariamente nuestro objeto social incluye la investigación, adiestramiento y formación como centro docente asistencial."[1]

1Sitio en Internet, Disponible en :
HTTP://HRPLOPEZ.GOV.CO/HOSPITAL/INDEX.PHP?OPTION=COM_FRONTPAGE&ITEMID=1

Con lo anterior la tecnología informática se erige como uno de los principales factores críticos del éxito de las organizaciones. Su aplicabilidad es cada vez mayor y las organizaciones dependen crecientemente de ella para la toma oportuna y confiable de sus decisiones; no obstante, el crecimiento informático en la mayoría de las empresas se realiza de forma no programada, es decir, no existe una planeación estratégica que determine la ruta tecnológica y el plan de inversiones. Las decisiones se toman de forma subjetiva cobijadas por planes que se trazan con extensión de un año.

Por otro lado los procedimientos para la gestión de servicios de TI se encuentran en su mayoría indocumentados lo que los torna informales y poco eficientes en su atención y solución. Adicionalmente, como no existe un proceso de evaluación y priorización se genera una excesiva pérdida de tiempo por parte del Jefe de Sistemas.

La creación de estándares para la definición de estructuras administrativas que redunden en una eficiente y efectiva gestión de servicios es preocupación de asociaciones internacionales de profesionales, quienes ya han sido aplicados exitosamente a nivel mundial lo que les ha permitido ser catalogados dentro de las mejores prácticas.

Entidades del sector oficial en Colombia han desarrollado planes encaminados a construir un adecuado Modelo de Gobierno de TI con reconocido éxito. En el sector salud no se conoce aún ningún avance en este sentido, pero en este proyecto se desarrollo en la ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ sentará las bases para ello. Para así optimizar la ejecución del plan estratégico corporativo en la ESE HOSPITAL PUMAREJO DE LOPEZ a partir de la construcción de un adecuado plan estratégico de tecnología informática y la definición de un Sistema de Gestión de Servicios de TI ajustado a sus necesidades.

¿QUÉ ES ITIL?

"Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) se ha convertido en el estándar mundial de de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL es conocido y utilizado mundialmente. Pertenece a la OGC, pero es de libre utilización.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del coste, y el resto se invierte en el desarrollo del producto (u obtención). De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o

suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de coste aceptable".[2]

¿QUÉ ES ISO 20000?

"La norma ISO 20000 se concentra en la gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia - los problemas se clasifican, lo que ayuda a identificar problemas continuados o interrelaciones. La norma considera también la capacidad del sistema, los niveles de gestión necesarios cuando cambia el sistema, la asignación de presupuestos financieros y el control y distribución del software.

La norma ISO 20000 se denominó anteriormente BS 15000 y está alineada con el planteamiento del proceso definido por la IT Infrastructure Library (ITIL - Biblioteca de infraestructuras de tecnología de la información) de The Office of Government Commerce (OGC)."[3]

Planeación Estratégica

"La planeación estratégica es una herramienta administrativa que ayuda a incrementar las posibilidades de éxito cuando se quiere alcanzar algo en situaciones de incertidumbre y/o de conflicto (oposición inteligente).

Se basa en la administración por objetivos y responde prioritariamente la pregunta "Qué hacer". Situaciones como la creación o reestructuración de una empresa, la identificación, y evaluación de programas y proyectos, la formulación de un plan de desarrollo, la implementación de una política, la conquista de un mercado, el

2Sitio en Internet, Disponible en: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php
3 Sitio en Internet, Disponible en : http://www.es.sgs.com/es/iso_20000?serviceId=10009985&lobId=1998

posicionamiento de un producto o servicio, la resolución de conflictos, son ejemplos de casos donde la Planeación Estratégica es especialmente útil.

El método se respalda en un conjunto de conceptos del pensamiento estratégico, algunos de cuyos más importantes principios son:

Priorización del Qué ser sobre el Qué hacer: es necesario identificar o definir antes que nada la razón de ser de la organización, la actividad o el proceso que se emprende; lo que se espera lograr.

Priorización del Qué hacer sobre el Cómo hacerlo: identificar las acciones que conducen efectivamente a la obtención del objetivo. Se trata de anteponer la eficacia sobre la eficiencia.

Visión sistémica: la organización o el proyecto son un conjunto de subsistemas (elementos) que tienen una función definida, que interactúan entre sí, se ubican dentro de unos límites y actúan en búsqueda de un objetivo común. El sistema está inmerso dentro de un entorno (contexto) que lo afecta o determina y que es afectado por él. Los elementos pueden tener su origen dentro del sistema (recursos), o fuera de él (insumos).

Visión de proceso: Los sistemas son entes dinámicos y cambiantes; tienen vida propia.

Deben ser vistos y estudiados con perspectiva temporal; conocer su historia para identificar causas y efectos de su presente y para proyectar su futuro.

Visión de futuro: el pensamiento estratégico es proactivo; se adelanta para incidir en los acontecimientos. Imagina permanentemente el mañana para ayudar a construirlo o para acomodarse a él: es prospectivo

Compromiso con la acción y con los resultados: el estratega es no solamente un planificador; es un ejecutor, conocedor y experto que reflexiona, actúa y avalúa; es un gestor a quien le importa más qué tanto se logra que, qué tanto se hace.
Flexibilidad: se acomoda a las circunstancias cambiantes para no perder el rumbo La acción emergente es algo con lo que también se puede contar, así que la capacidad para improvisar es una cualidad estratégica.

Estabilidad: busca permanentemente un equilibrio dinámico que permita el crecimiento seguro, minimizando el riesgo y la dependencia. Busca la sostenibilidad del sistema y de los procesos.
La Planeación Estratégica es un proceso de cuatro etapas en las que se van definiendo uno a uno los siguientes interrogantes:

¿Qué se quiere lograr?
¿En qué situación se está?
¿Qué se puede hacer?
¿Qué se va a hacer?4

Gobierno de TI.

"El término Gobierno de TI no es una frase común dentro de las conversaciones entre los profesionales de tecnologías de información y mucho menos fuera del entorno de tecnología. Sin embargo, su concepto es muy valioso ya que producto de una correcta implementación de un modelo de Gobierno de TI, habilita a la organización receptora con las herramientas necesarias para tomar decisiones óptimas respecto a la realización de inversiones en tecnología considerando la dirección, requerimientos del negocio y su comportamiento financiero.

4 Sitio en internet, Disponible en:
http://www.virtual.unal.edu.co/cursos/agronomia/2008868/lecciones/capitulo_2/cap2lecc2.htm

Asimismo, otras ventajas importantes de la implantación de un modelo de Gobierno de TI son: Maximizar el valor agregado al negocio por parte de las inversiones en TI, y Monitorear y dar seguimiento de la realización del beneficio inicialmente estimado para dichas inversiones. Una mala inversión en TI puede tener un alto impacto en los planes de negocio de la organización.

Gobierno de TI puede también ser definido como una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la empresa y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos.

El núcleo de TI consta de dos responsabilidades principales, la entrega de valor al negocio y mitigar los riesgos relacionados con TI. La gerencia de la organización necesita ampliar sus responsabilidades de gobierno a TI y proveer estructuras y procesos que aseguren que las Tecnologías de Información son capaces de soportar los objetivos y estrategias de la organización. Cada implementación de gobierno de TI se lleva a cabo en diferentes condiciones y circunstancias (entorno de Gobierno de TI) determinados por factores tales como:

- Ética y cultura de la organización y de la industria.
- Leyes, regulaciones y guías vigentes, tanto internas como externas.
- Misión, visión y valores de la organización.
- La organización de la organización de sus roles y responsabilidades.
- Intenciones estratégicas y tácticas de la organización."[5]

5 Sitio en Internet, Disponible en : http://www.deloitte.com/view/es_PE/pe/servicios/consultoria/tecnologia-de-la-informacion/gobierno-de-ti/index.htm

6. DISEÑO METODOLÓGICO

Con base en los lineamientos establecidos por ITIL el equipo del proyecto diseñará instrumentos para evidenciar para cada gestión del Modelo cuales servicios ofrece actualmente la Institución y su coherencia con el deber ser.

El equipo del proyecto efectuará un levantamiento de información que se plasmará en documentos de análisis que posteriormente constituirán la base de la propuesta que se presentará.

Se efectuará investigación sobre muestras representativas de entidades de salud de los sectores públicos y privados con el objeto de establecer el grado de avance que se tiene, en este tipo de instituciones, con respecto al dominio y estructuración de la gestión de servicios.

Con esta información se efectuará una triangulación para cotejar lo expuesto por los estándares, lo que dicen los académicos y lo existente en el mercado. Los resultados constituirán el fundamento para definir el nivel de maduración que se pretenda alcanzar para el modelo de Gestión de Servicios de TI.

Esta investigación es socio crítico, porque “introduce la ideología de forma explicita y la autorreflexión critica en los procesos del conocimiento. Sus principios ideológicos tienen como finalidad la transformación de la estructura de las relaciones sociales. Esta perspectiva tiene como objetivo el análisis de las transformaciones sociales y dar respuesta a determinados problemas generados por estas.”; también Permite identificar las razones que generan los cambios en el comportamiento de los grupos sociales. En razón a estos fundamentos se considera adecuado para este proyecto de investigación.

En esta investigación se emplea un enfoque etnográfico, porque el propósito fundamental de este tipo de estudio es describir un grupo humano o algún aspecto de

una o más culturas en una organización, ya que la característica relevante en la Etnografía es que incorpora las experiencias, creencias, actitudes, pensamientos, reflexiones, de los participantes.

El paradigma cualitativo fundamenta esta investigación, La investigación cualitativa, es aplicable a este trabajo en razón a que el enfoque cualitativo conocido también como "fenomenológico, naturalista, humanista, o etnográfico, engloba un conjunto de corrientes humanísticos-interpretativas cuyo interés se centra en el estudio de los significados de las acciones humanas y de la vida social"6 y en este sentido se presentan descripciones de observación y entrevista de preguntas abiertas en los cuales se muestra las tendencias que conllevan a un análisis de los datos, para obtener los resultados que se pretende mostrar.

La población objeto de estudio de esta investigación está representada por el Hospital rosario Pumarejo de López Valledupar, compuesta por los directivos, funcionarios.
Como técnica de recolección de información se emplearan la entrevista y la observación. Con la entrevista a los funcionarios, directivos se pretende precisar la estructura organizativa y procedimientos para la óptima gestión de servicios de TI y Con la observación se busca analizar el funcionamiento actual ofrecido por el área de informática para diseñar un plan estratégico de Tecnología Informática alineado con el Plan estratégico corporativo.

6 (ERICKSON, 1986); Citado por: Documento PEÑA, Judith, Naturaleza de la Investigación, p 40 - 41.

CAPITULO I

7. GENERALIDADES DE LOS ESTÁNDARES INTERNACIONALES

7.1 Antecedentes Sobre las Normas Técnicas y Estándares Internacionales

Las entidades de salud encaminadas a prestar un servicio óptimo a la comunidad o a los interesados (stakeholders) y al entorno en general a través de los sistemas de información, que les apoyen para obtener un mayor beneficio, aumentar el volumen de sus transacciones, tener una mayor cobertura, prestar servicios de calidad, brindar un ambiente laboral adecuado y de aprendizaje y crecimiento para sus empleados, es necesario que las entidades de salud cuenten con una planeación que le ayuden al logro de sus objetivos. Estos procesos se construyen con la participación de todos los miembros de la organización, involucrándolos en cada unos de ellos, es así que la planeación estratégica en sistemas de información es vital para conocer el horizonte en el área de sistemas que le permitan implementar estrategias que se alineen con los objetivos del negocio y sirvan de apoyo a todas las áreas de la organización para el cumplimiento de plan estratégico institucional. Destacando cuatro estándares para la construcción de un modelo de Gobierno de TI y que gozan de gran aceptación mundial, por lo que han sido denominados como “Mejores Prácticas”, estos son:

a. COBIT 4.1.: Marco de referencia para el Gobierno de TI, como el de mejores lineamientos para el diseño de un gobierno de TI.
b. Norma ISO 27001 e ISO 27002. : Sistema de Gestión de la Seguridad de la Información.
c. Norma ISO 20000.: Estandard para certificar la Gestión de Servicios de TI de las Empresas y Organizaciones.

d. ITIL: Estándar para la Gestión de Servicios de TI.

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales.

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI de la empresa sirve como base a los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte al Committee Of Sponsoring Organisations Of The Treadway Commission *Control interno—Marco de Referencia integrado*, el marco de referencia de control ampliamente aceptado para gobierno de la empresa y para la administración de riesgos, así como a marcos compatibles similares.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para la TI y decidir qué tipo de gobierno y de control debe aplicar.

***Los Objetivos de Control para la Información y la Tecnología relacionada* (COBIT®)** brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

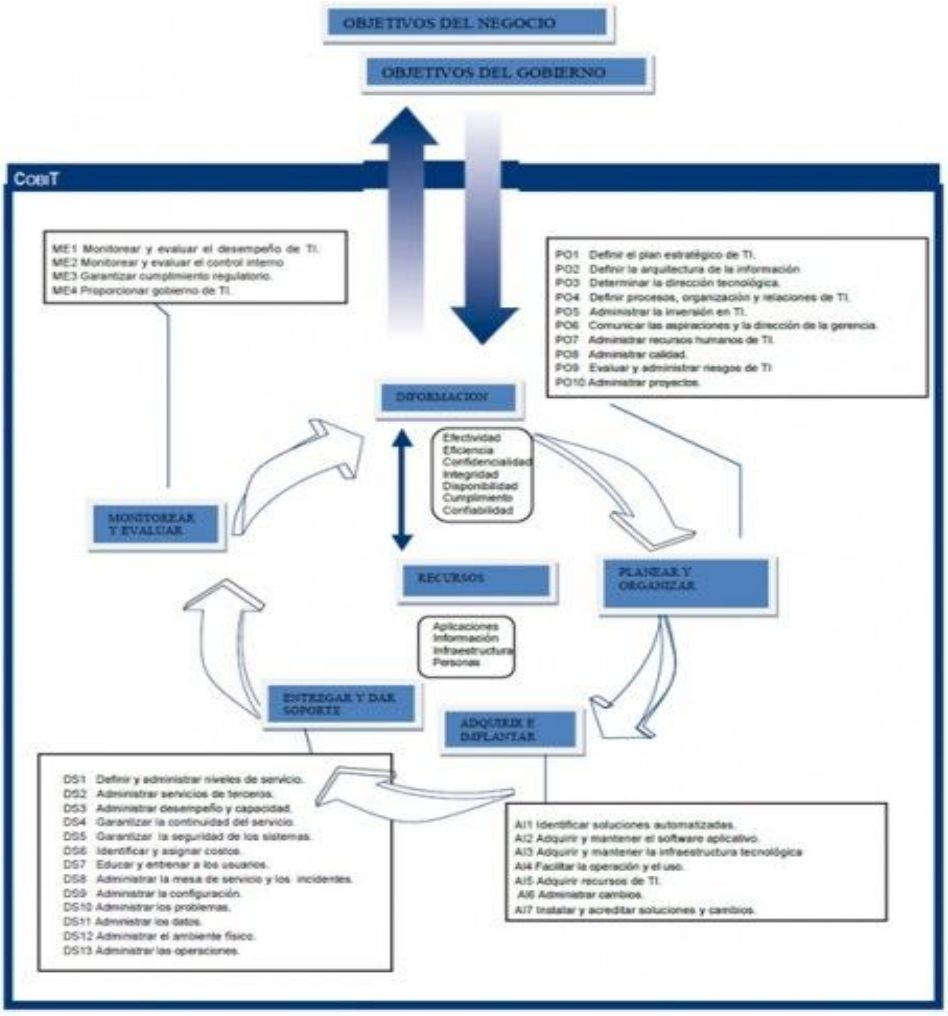
Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implantar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio.
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado.
- Identificando los principales recursos de TI a ser utilizados.
- Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en vincular las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, compuesto de cuadro dominios el cual contienen 34 procesos genéricos, de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. (Ver Figura 1). Administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

FIGURA 1. MARCO DE TRABAJO GENERAL DE COBIT



Fuentes: IT Governance Institute, Cobit 4.1 – Isaca

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

Pero, ¿cómo puede la empresa poner bajo control la TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio?

Primero, la dirección requiere objetivos de control que definan la última meta de implantar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un nivel razonable para garantizar que:

- Se alcancen los objetivos del negocio.
- Se prevengan o se detecten y corrijan los eventos no deseados.

En segundo lugar, en los complejos ambientes de hoy en día, la dirección busca continuamente información oportuna y condensada, para tomar decisiones difíciles respecto a riesgos y controles, de manera rápida y exitosa. ¿Qué se debe medir y cómo? Las empresas requieren una medición objetiva de dónde se encuentran y dónde se requieren mejoras, y deben implantar una caja de herramientas gerenciales para monitorear esta mejora.

Una respuesta a los requerimientos de determinar y monitorear el nivel apropiado de control y desempeño de TI son las definiciones específicas de COBIT de los siguientes conceptos:

Benchmarking de la capacidad de los procesos de TI, expresada como modelos de madurez, derivados del Modelo de Madurez de la Capacidad del Instituto de Ingeniería de Software.

Metas y métricas de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de balanced business Scorecard de Robert Kaplan y David Norton.

Metas de actividades para controlar estos procesos, con base en los objetivos de control detallados de COBIT.

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelado de la madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.

COBIT da soporte al gobierno de TI (Ver Figura 2) al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI capacita el negocio y maximiza los beneficios
- Los recursos de TI se usen de manera responsable
- Los riesgos de TI se administren apropiadamente.

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de la medición del desempeño.

FIGURA 2. AREAS FOCALES DEL GOBIERNO DE TI

Fuentes: IT Governance Institute, Cobit 4.1 – Isaca

Alineación Estratégica se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de Valor se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

Administración de Recursos se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI, aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

Administración de Riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Medición del Desempeño rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.[7]

[7] IT Governance Institute, Cobit 4.1 – Isaca

El GOBIERNO DE TI que es el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. Se constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que TI soporta y facilita el desarrollo de los objetivos estratégicos definidos.

Garantizando que:

- TI está alineada con la estrategia del negocio.
- Los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente.
- Todos los riesgos relacionados con TI son conocidos y administrados y los recursos de TI están seguros.

Marco de Referencia

Es un conjunto de métodos y prácticas que permiten establecer:

- Criterios de información exigidos por los requisitos de negocio.
- Procesos de negocio.
- Recursos a utilizar.

Sus características son:

- Está orientado a procesos, tanto de TI como del negocio. Se debe definir el propietario del proceso, la responsabilidad sobre el proceso y la criticidad del mismo.
- Basado en prácticas comúnmente aceptadas para aprovechar la experiencia del mercado y ofrecer un conjunto de medidas de control multinacional, hecho especialmente importante para la auditoría.

IT Governance: ITIL, COBIT, CMMI

- Utiliza un lenguaje común debido a la tradicional ausencia de comunicación entre negocio y tecnología. Se deben comprender los procesos y la complejidad de los recursos TI.
- Permite la adopción de requisitos regulatorios.

Necesidad del Marco de Trabajo

- Asegurar el alineamiento con los objetivos de la organización.
- Determinar y mitigar los riesgos empresariales.
- Asegurar el cumplimiento normativo de forma general.
- Calcular/proveer formalmente los recursos apropiados.
- Hacer el seguimiento de la aportación de las TI al negocio.

Métricas

Los marcos de control están dirigidos por medidas. El negocio necesita conocer el estado de sus recursos y procesos TI, cómo aportan valor y cómo evolucionan. Sirvan como ejemplo:

Key Performance Indicator: Cómo se llega al grado de cumplimiento.

CMM: Es un modelo de evaluación de los procesos de una organización. Cada proceso evaluado por CMM define un conjunto de buenas prácticas que habrán de ser: definidas en un procedimiento, provistas de los medios y formación necesarios, ejecutadas de un modo sistemático, universal y uniforme, medidas y verificadas. En función del estadio de aplicación de cada práctica, el proceso se clasifica en: **Inicial / Repetible / Definido / Gestionado / Optimizado.**

IT Governance: ITIL, COBIT, CMMI.

BSC (Cuadro de Mando Integral): El "Cuadro de Mando Integral" es una herramienta para la gestión del rendimiento organizativo. Ayuda a centrarse no sólo en los objetivos financieros, sino también en los procesos internos, en los Clientes, y en los aspectos relativos al crecimiento y aprendizaje. Debería encontrarse un equilibrio entre estas cuatro perspectivas.

Las cuatro perspectivas se centran en las siguientes cuestiones:

- Clientes: ¿Qué desean nuestros Clientes?
- Los procesos internos: ¿Cómo proporcionamos a nuestros Clientes un valor añadido?
- Aprendizaje y crecimiento: ¿Cómo garantizamos que seguiremos generando valor añadido en el futuro?
- Los aspectos financieros: ¿Qué tal lo hicimos en términos financieros?

El **Gobierno TI** es el único camino posible para asegurar que las áreas de sistemas contribuyen al éxito de las empresas en las que se encuadran, realizando una gestión más eficiente de los recursos, minimizando los riesgos y alineando sus decisiones con los objetivos del negocio.
IT Governance: ITIL, COBIT, CMMI

Los factores inductores del Gobierno TI en la organización pueden ser:

- **Regulaciones y Normativa:** Legales (SOX, LOPD), Estándares (ISO 27001, ISO 20000), Certificaciones CMMI.
- **Optimización de Recursos:** Reingeniería procesos TI, Consolidación de Recursos, Estrategias de externalización.

- **Peticiones del Negocio:** Alineamiento TI con la estrategia, Ciclo de vida de productos y servicios, gestión de la demanda.

Los Factores Críticos Pueden ser los Siguientes:

- Conocer dónde se desea ir, evitando siempre la improvisación.
- Establecer mecanismos de medición y control claros.
- Que el marco temporal sea adecuado, la mejora lleva tiempo, no se deben esperar resultados a corto plazo, en menos de seis meses.
- Alinearse con iniciativas que ya estén en curso.
- No perderse en los modelos, no hay modelo ideal, cada situación requiere de soluciones a medida.
- Dotar a la organización de herramientas adecuadas.[8]

Norma ISO 27001 e ISO 27002. : Sistema de Gestión de la Seguridad de la Información.

La norma ISO 27001 e ISO 27002, sirven para garantizar el sistema de Gestión de la Seguridad de la información que servirá para que la organización tenga salvaguardado su sistema de información.

El estándar para la seguridad de la información **ISO/IEC 27001** (*Information technology - Security techniques - Information security management systems - Requirements*) fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo

[8] Gobierno de TI - TCP Sistemas e Ingeniería, http://www.tcpsi.com/servicios/gobierno_ti.htm

de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar).

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) elegido. En general, es recomendable la ayuda de consultores externos.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI).[9]

El ISO/IEC 27002, estándar internacional fue publicado por la ISO (*www.iso.org/ISO/home.htm*) y la IEC, que establecieron el comité técnico mixto ISO/IEC JTC 1. La fuente histórica para el estándar fue BS 7799-1, cuyas partes esenciales fueron tomadas en el desarrollo de la norma ISO/IEC 17799:2005 Tecnología de la Información – Código de Prácticas para la Gestión de Seguridad de la Información.

El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para

[9] ISO/IEC 27001, http://es.wikipedia.org/wiki/ISO/IEC_27001

mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

Los principios rectores en la norma ISO/IEC 27002:2005 son los puntos de partida para la implementación de seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.[10]

ISO/IEC 20000

A partir del 14 de Diciembre de 2005, Es reconocido mundialmente como un estandard para certificar la Gestión de Servicios de TI de las Empresas y Organizaciones, **ISO/IEC 20000** (International Organization for Standardization) e IEC (International Electrotechnical Commission).

La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización y certificación británica BSI (British Standard Institute).

El Estándar Comprende dos partes:

- **Parte 1**: ISO/IEC 20000 - 1: 2005 - **Especificación**. (Preparada por BSI como BS 15000 -1).
- **Parte 2**: ISO/IEC 20000 - 2: 2005 - **Código de Prácticas**. (Preparada por BSI como BS 15000 - 2).

[10] **Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa,** IT Governance Institute, Isaca

La Primera Parte (Especificación):

Define los requerimientos necesarios (217) que deben cumplirse para realizar la entrega de servicios de TI alineados con la Visión y Objetivos del Negocio, integrando así las distintas áreas de la organización con calidad y valor agregado para los clientes, asegurando una optimización de los costes y garantizando la seguridad de la entrega en todo momento.

El cumplir con esta especificación es garantía de que la organización cuenta con un "Ciclo de Mejora Continua" de la Gestión de los servicios de TI que ofrece.

Este Estándar Internacional Comprende los Siguientes Procesos:

- Grupo de Procesos de Provisión del Servicio.
- Grupo de Procesos de Control.
- Grupo de Procesos de Entrega.
- Grupo de Procesos de Resolución.
- Grupo de Procesos de Relaciones.

La Segunda Parte (*Código de Prácticas*) ITIL :

Representa el conjunto de Mejores Prácticas "adoptadas" y "aceptadas" por la industria en materia de Gestión de Servicio de TI. Está basada en el estándar mundial para el área de IT (ITIL (Biblioteca de Infraestructura de TI) que sirve como guía y base para la definición de nuevas acciones de mejora de los servicios en el servicio o preparación de auditorías contra el estándar ISO/IEC 20000 - 1:2005.

La especificación supone un completo sistema de gestión (organizado según ISO 9001) basado en procesos de gestión de servicios, políticas, objetivos y controles.

ITIL (PROPIEDAD DE LA OGC DE INGLATERRA | OFFICE OF GOVERMENT OF COMMERCE).

ITIL (Information Technology Infrastructure Library), es el estándar internacional adoptado por las principales empresas de servicios a nivel mundial, para reducir costos y optimizar los servicios que ofrecen a través del área de TI, aumentando la disponibilidad y calidad de los mismos.

ITIL es un Framework, documentado en un conjunto de libros, que conforman la Biblioteca de Mejores Prácticas que permiten mejorar notablemente la calidad de los servicios de tecnologías de la información que presta una empresa a sus clientes o un departamento de su organización.[11]

En el documento Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa, IT Governance Institute, Isaca, Las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

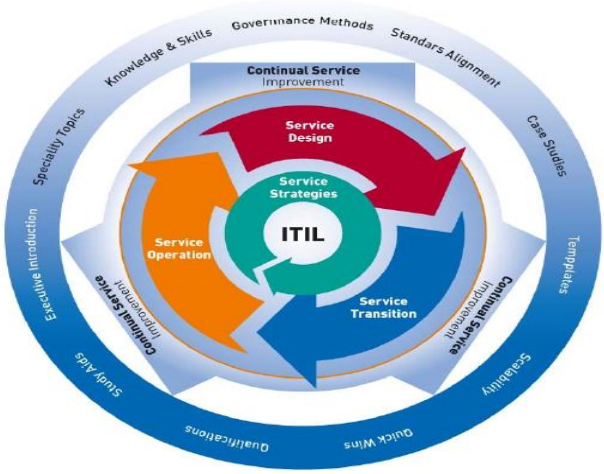
- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de
servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI. ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este

[11] Introducción ISO20000 COLOMBIA, http://www.iso20000.com.ar/intro_col.html

contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse. Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima. Ver Figura 3.

FIGURA 3. APORTE DE ITIL AL GOBIERNO DE TI



Fuente: Euro Portal de Servicios

ITIL - Expertos en Gestión Informáticos

VENTAJAS DE IMPLANTAR ITIL[12]

A. Estrategia Del Servicio.

- Al conocer como es el mercado podrá establecer nuevos servicios a partir de las tecnologías con las que cuente.
- Al conocer el mercado disminuye los errores entre lo que le ofrezco, y sus verdaderas necesidades.

B. Diseño Del Servicio

- El tener claro que tipo de servicio ofrezco y los insumos que necesito, permite que siempre tenga provisión y evita que en algún momento, pueda fallar el servicio al cliente.
- También será posible identificar que falencias a largo plazo, se podrán presentar en el caso de que no cuente con todos los recursos para la prestación de un servicio.
- Se podrá identificar a que es lo que realmente se puede dedicar, que puede hacer sin fallar.
- Dependiendo de las necesidades del cliente podría conseguir nuevos insumos, para dar un servicio más integral.

[12] Paramo Díaz, Harol André. Proyecto Implementación ITIL. En: Scridb. [en línea]. [consultado 28 de Noviembre 2011]. Disponible en http://es.scribd.com/doc/57366549/Actividad-de-Itil#archive, p 16

C. Transición del Servicio

- Disminuir las posibles fallas que se pueden presentar al implementar un servicio.
- Disminuir los costos que pueden acarrear las fallas que se presenten por falta de previsión.
- Garantizar que los datos y procesos importantes de una empresa, no se pierda, si no que entren en el nuevo ciclo de servicios de la empresa.

D. Operación Del Servicio

- Tener claridad de los tiempos y los costos de los procesos, puede lograrse una mayor calidad en las prestación de servicios.
- A la hora de ajustar precios, se podrá ver con precisión, que procesos e implementos pueden sobrar a la hora de prestar un servicio específico.

E. Mejora del Servicio

- Al tener una medición exacta de los procesos, puede mirar con claridad cuales pueden quedar obsoletos, cuales me están generando carga.
- Al recibir las sugerencias tanto internas como externas, podrá cada vez mejorar el servicio hasta llegar a convertirse en una empresa que ofrece calidad.

PRINCIPALES PROCESOS QUE SE LLEVAN A CABO EN LOS SERVICIOS DE LA EMPRESA CON ITIL[13]

a. Procesos de la Mesa de Ayuda

- Atender la llamada de los clientes según guion preestablecido.
- Alimentar una base de datos que pueda ser consultada por los asesores que presten el servicio.
- Instalar en la base de datos las mejoras de acuerdo a las sugerencias internas y externas.
- Hacer capacitaciones para que el personal encargado entienda perfectamente los temas.
- Contratación de personal calificado.

b. Procesos de Mantenimiento de Hardware

- Verificación de insumos en la bodega.
- Contratación de personal calificado.
- Preparación del personal respecto a los procesos.
- Asistir al mantenimiento dentro del tiempo establecido.
- Reportar novedades, fallos o insumos que falten a jefe inmediato.

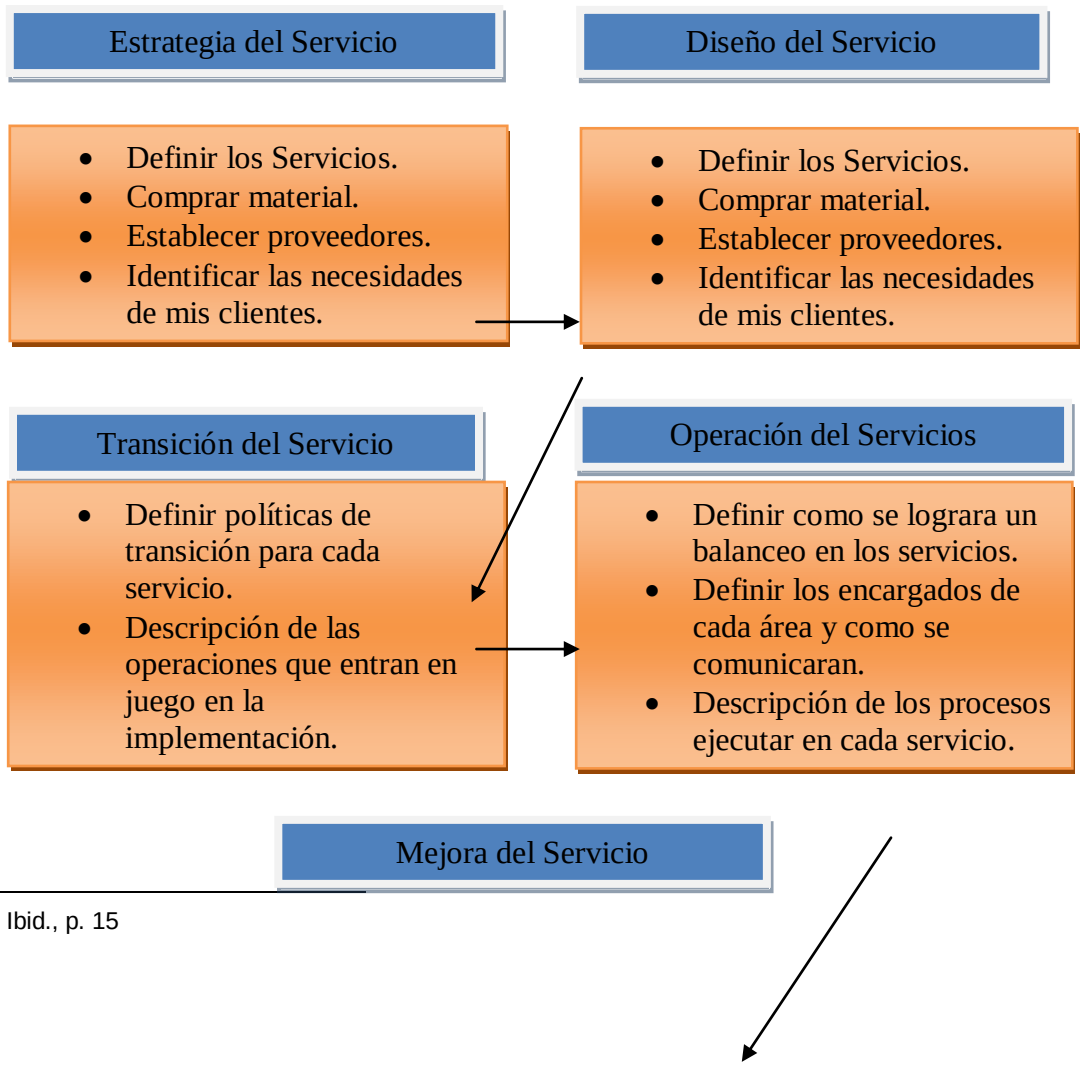
[13] Ibid., p. 14

c. Procesos Administración de Servidores

- Asistir al cliente en el horario asignado en la mesa de ayuda.
- Asistir a nuevos cursos para informarse de nuevas tecnologías.
- Documentar las fallas y las soluciones

d. Procesos de Entrenamiento de TI.

FIGURA 4. ESQUEMA DE IMPLEMENTACION DE ITIL PARA LA EMPRESA[14]



[14] Ibid., p. 15

- Establecer el encargado del.
- Establecer medios para recibir sugerencias.
- Establecer mediciones para mejora del servicio.

DOCUMENTACION MINIMA REQUERIDA PARA EL CONTROL DE LA GESTION DE LA EMPRESA[15]

- Un documento donde detalle los activos, los proveedores
- Un documento donde se describe el guion que deben seguir la persona de mesa de ayuda.
- Documentos para cada área donde están registradas las sugerencias internas y externas.
- Un documento donde describa los tipos de servicio que va a ofrecer.
- Documentos donde describa todos los insumos que necesita la empresa en cada área.
- Documento donde describe las políticas de transición de la empresa.
- Documento donde describe las funciones de cada empleado en cada área.
- Un documento donde describa los procesos de operación del servicio.
- Hojas de vida cada uno de los que laboran en la empresa.
- Documento donde se describe los insumos que faltan en determinada área.
- Documento donde se describan fallas y soluciones.
- Documento donde se describan fallas y soluciones.
- Un documento donde se muestran las fallas y soluciones en el área requerida.

[15] Ibid., p. 17

EL MODELO CMMI

El Nacimiento de CMM - CMMI

El departamento de defensa de los estados unidos tenía muchos problemas con el software que encargaba desarrollar a otras empresas, los presupuestos se disparaban, las fechas alargaban más y más. ¿Quién no se ha encontrado con este tipo de problemas si ha trabajado con una empresa de software?

Como esta situación les parecía intolerable convocó un comité de expertos para que solucionase estos problemas, en el año 1983 dicho comité concluyó "Tienen que crear un instituto de la ingeniería del software, dedicado exclusivamente a los problemas del software, y a ayudar al Departamento de Defensa".

Convocaron un concurso público en el que dijeron: "Cualquiera que quiera enviar una solicitud tiene que explicar como van a resolver estos 4 problemas", se presentaron diversos estamentos y la Universidad Carnegie Mellon ganó el concurso en 1985, creando el SEI.

El SEI (Software Engineering Institute) es el instituto que creó y mantiene el modelo de calidad CMM - CMMI

¿Qué es el CMM - CMMI?

El CMM - CMMI es un modelo de calidad del software que clasifica las empresas en niveles de madurez. Estos niveles sirven para conocer la madurez de los procesos que se realizan para producir software.

Niveles CMM - CMMI

Los niveles CMM - CMMI son 5:

- **Inicial o Nivel 1 CMM - CMMI**. Este es el nivel en donde están todas las empresas que no tienen procesos. Los presupuestos se disparan, no es posible entregar el proyecto en fechas, te tienes que quedar durante noches y fines de semana para terminar un proyecto. No hay control sobre el estado del proyecto, **el desarrollo del proyecto es completamente opaco**, no sabes lo que pasa en él.

  Es el típico proyecto en el que se da la siguiente situación:

  - ¿Cómo va el proyecto?
  -Bien, bien. Dos semanas después…
  - ¿Cómo va el proyecto?
  - Bien, bien. Tres semanas después…

  - El lunes hay que entregar el proyecto.- No se por qué pero los proyectos se entregan los lunes.
  - El lunes? Todavía falta mucho!!
  - ¿Cómo? Me dijiste que el proyecto iba bien!! Arréglatelas como quieras, pero el proyecto tiene que estar terminado para el lunes.

  Si no sabes el tamaño del proyecto y no sabes cuanto llevas hecho, nunca sabrás cuando vas a terminar.

Repetible o Nivel 2 CMM - CMMI. Quiere decir que el éxito de los resultados obtenidos se pueden repetir. La principal diferencia entre este nivel y el anterior es que **el proyecto es gestionado y controlado durante el desarrollo** del mismo. El desarrollo no es opaco y se puede saber el estado del proyecto en todo momento.

Los procesos que hay que implantar para alcanzar este nivel son:

- Gestión de requisitos
- Planificación de proyectos
- Seguimiento y control de proyectos
- Gestión de proveedores
- Aseguramiento de la calidad
- Gestión de la configuración

- **Definido o Nivel 3 CMM - CMMI**. Resumiéndolo mucho, este alcanzar este nivel significa que la **forma de desarrollar proyectos (gestión e ingeniería) esta definida**, por definida quiere decir que esta establecida, documentada y que existen métricas (obtención de datos objetivos) para la consecución de objetivos concretos.

  Los procesos que hay que implantar para alcanzar este nivel son:

  - Desarrollo de requisitos
  - Solución Técnica
  - Integración del producto
  - Verificación
  - Validación

- Desarrollo y mejora de los procesos de la organización
- Definición de los procesos de la organización
- Planificación de la formación
- Gestión de riesgos
- Análisis y resolución de toma de decisiones

La mayoría de las empresas que llegan al nivel 3 paran aquí, ya que es un nivel que proporciona muchos beneficios y no ven la necesidad de ir más allá porque tienen cubiertas la mayoría de sus necesidades.

- **Cuantitativamente Gestionado o Nivel 4 CMM - CMMI**. Los proyectos usan objetivos medibles para alcanzar las necesidades de los clientes y la organización. Se usan métricas para gestionar la organización.

  Los procesos que hay que implantar para alcanzar este nivel son:

  - Gestión cuantitativa de proyectos
  - Mejora de los procesos de la organización

- **Optimizado o Nivel 5 CMM - CMMI**. Los procesos de los proyectos y de la organización están orientados a la mejora de las actividades. Mejoras incrementales e innovadoras de los procesos que mediante métricas son identificadas, evaluadas y puestas en práctica.

  Los procesos que hay que implantar para alcanzar este nivel son:

  - Innovación organizacional
  - Análisis y resolución de las causas

Normalmente las empresas que intentan alcanzar los niveles 4 y 5 lo realizan simultáneamente ya que están muy relacionados.

A grandes rasgos os he intentado introducir el modelo de calidad del software CMM - CMMI para aquella gente que se encuentra por primera vez con él. **La implantación de un modelo de estas características es un proceso largo y costoso que puede costar varios años de esfuerzo.** Aun así el beneficio obtenido para la empresa es mucho mayor que lo invertido. [16]

"Y a este respecto se debe tener en cuenta hasta qué punto no hay cosa más difícil de tratar, ni más dudosa de conseguir, ni más peligrosa de conducir, que hacerse promotor de la implantación de nuevas instituciones.

La causa de tamaña dificultad reside en que el promotor tiene por enemigos a todos aquellos que sacaban provecho del viejo orden y encuentra unos defensores tímidos en todos los que se verían beneficiados por el nuevo.

Esta timidez nace en parte al temor de los adversarios, que tienen la ley de su lado, y en parte también la incredulidad de los hombres, quienes -en realidad- nunca creen en lo nuevo hasta que adquieren una firme experiencia en ello.

De ahí nace que, siempre que los enemigos encuentran la ocasión de atacar, lo hacen con ánimo faccioso, mientras los demás sólo proceden a la defensa con tibieza, de lo cual resulta un serio peligro para el príncipe y para ellos."

El Príncipe, Nicolás Maquiavelo, 1513

[16] Gracia, Joaqui. CMM – CMMI. En: IngenieroSoftware. [en línea]. 14 de Agosto de 2005. [consultado 28 de noviembre 2011]. Disponible en http://www.ingenierosoftware.com/calidad/cmm-cmmi.php

FIGURA 5. EL MODELO CMMI

CAPITULO II

8. DIAGNOSTICO DE TI DE LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ A TRAVES DE LOS MODELOS DE MADURES. (CMMI)

Como fuente primaria para la realización de un diagnostico del área de Tecnología Informática de la ESE Hospital Rosario Pumarejo de López, se realizaron tres (3) listas de chequeo, enfocadas a evaluar el control y Gobierno de TI, la seguridad de la información, y concomimiento de las aplicaciones, la infraestructura de tecnológica y servicios de TI en la ESE, apoyándonos en las mejores prácticas como COBIT, ISO/IEC - 27001, ISO/IEC – 27002, ITIL V3 E ISO 27000.

8.1 Diagnostico En Base al Gobierno de Ti – COBIT 4.1

El siguiente fue el instrumento de recolección de información basado en COBIT para diagnosticar el estado del arte en gobierno de TI del área de sistemas de la ESE Hospital Rosario Pumarejo de López. Ver Anexo 1

Como resultado de la aplicación del instrumento de recolección basado en los dominios y objetivos de control COBIT 4.1, diligenciado en el Hospital Rosario Pumarejo de López los días 5, 6, 18 y 19 de julio de 2011 a manera de entrevista con el ingeniero de Sistemas y/o Director del Área de TI de la ESE Hospital Rosario Pumarejo de López podemos diagnosticar que:

El área de TI de la ese Hospital Rosario Pumarejo de López, tiene conciencia y reconoce de la importancia de diseñar e implementar un Plan Estratégico de Tecnología informática, que este alineado con el Plan de Gestión Institucional para el logro de los

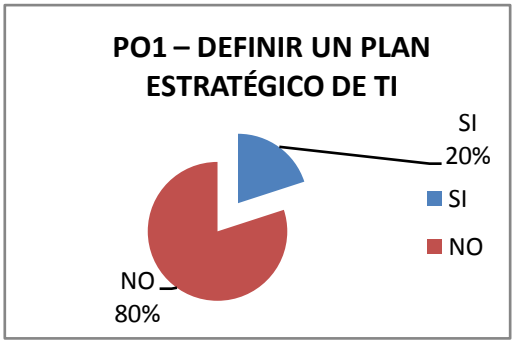
objetivos de negocio y brindar valor agregado a la organización, no obstante se observa que para planear la dirección tecnología, definir y determinar los procesos de TI, administrar recursos y riesgos de TI, son muy escasos los documentos de procedimientos formales apoyados en las buenas prácticas, tanto para su implementación como para su gestión; el Dominio Adquirir, e Implementar, no se gestiona de la mejor manera, porque se carece de una metodología clara para la identificación y la evaluación de las soluciones de TI que se quieren adquirir, ausencia de esquemas de procedimientos para la realización de mantenimientos, no se tienen implementado procedimientos y planes de gestión de cambios, los ambientes de producción y de certificación no están separados, no existe un proceso definido de adquisición de recursos de TI, No existe un proceso que defina y administre los niveles de servicio del área de TI y no se realiza una gestión de incidentes.

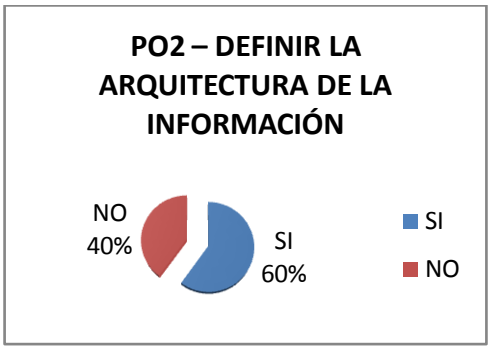
El dominio Entregar y dar Soporte, pese a que existen políticas y procedimientos para la contratación con terceros bien definidos, los contratos de soporte técnico que se encuentran tercerizados, tienen asignado una responsable de la supervisión y cumplimiento de lo contratado, pero el perfil de esta persona no le ayuda en el desarrollo de esta labor, ya que se podría realizar un trabajo más objetivo en la medida en que la persona que haga supervisión o seguimiento de los contratos de soporte técnico, mantenimiento preventivo y/o correctivo de equipos y acuerdos de servicio del área de TI tuviera un perfil tecnológico. A demás no están definidos acuerdos de niveles de operación, entre las diferentes áreas y TI; la evaluación que se hace de los acuerdos de niveles de servicio con terceros es muy global, y no se llevan registro de todas las solicitudes de soporte realizadas por las diferentes áreas, que permitan evaluar el grado de satisfacción de la calidad del servicio prestado, y el tiempo de repuesta para solucionar el incidente; no se realiza un seguimiento efectivo a la calidad del servicio prestado; no hay registro de las solicitudes de servicio más frecuentes; no existe una mesa de ayuda que permita realizar las tareas de soporte por parte de terceros, de una manera más eficiente, permitiendo la priorización, y la escalabilidad del servicio cuando este lo amerite; no se realiza una administración del desempeño y la

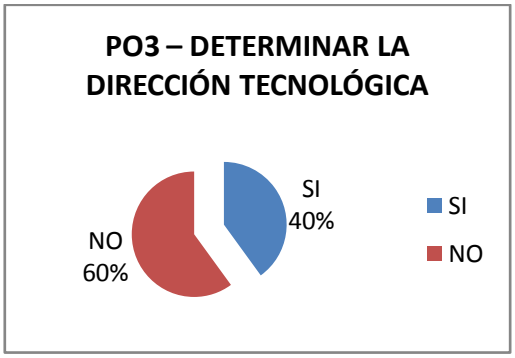
capacidad de TI; La ESE Hospital Rosario Pumarejo de López cuenta con una política y procedimiento para la realización de Backup, no obstante no tiene implementado un plan de continuidad de TI; no se han identificados y asignados costos de recursos de TI; la capacitación que se realiza a los usuarios es my puntual y generalmente cubre aspectos del manejo del aplicativo Dinámica Gerencial y correo electrónico; no existe un procedimiento que permita administrar la configuración de la infraestructura de TI, tanto a nivel de software como a nivel de hardware , es decir no existe un repositorio de configuraciones completo y preciso en donde están documentadas las configuraciones iniciales y/o ideales, de equipos activos de red, servidores, y aplicativos, ya que estos conocimientos están concentrados en el Gerente de TI y el ingeniero encargado de administrar el Call Center; no hay una adecuada gestión de incidentes y problemas, pero en la ESE si existe una adecuada administración del ambiente físico.

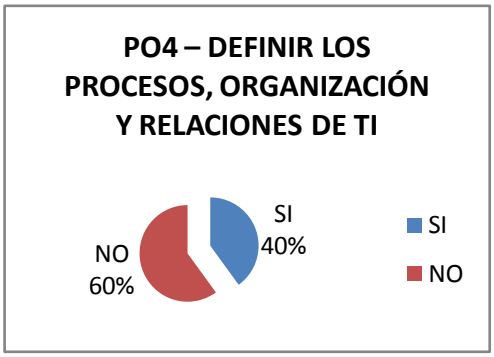
En cuanto al Dominio Monitorear y evaluar, en la ESE Hospital Rosario Pumarejo de López, no se mide el desempeño de TI, ni existen métricas para medir el nivel de satisfacción de los usuarios TI, no obstante la oficina de Control Interno fundamentada en los principios y objetivos institucionales “Creciendo para todos con Calidad” y apoyada en las herramientas de gestión MECI, SGC y SOGC, realiza monitoreo y evalúa el control interno y el cumplimiento de los requisitos legales, contractuales y regulatorios.

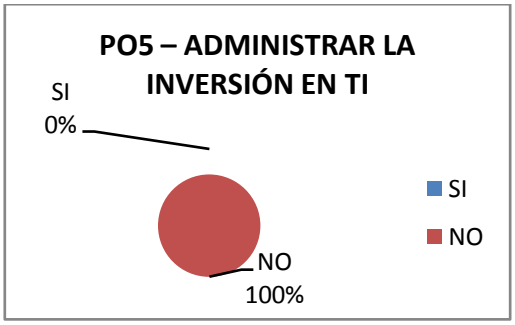
Las siguientes graficas muestran el nivel de cumplimiento de los procesos COBIT por la ESE Hospital Rosario Pumarejo de López.


PO1 – DEFINIR UN PLAN ESTRATÉGICO DE TI
SI 20%
NO 80%
SI
NO

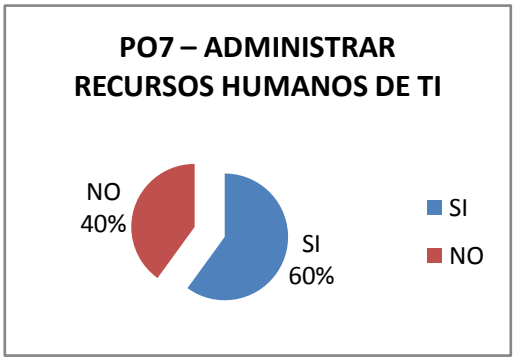

PO2 – DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
NO 40%
SI 60%
SI
NO

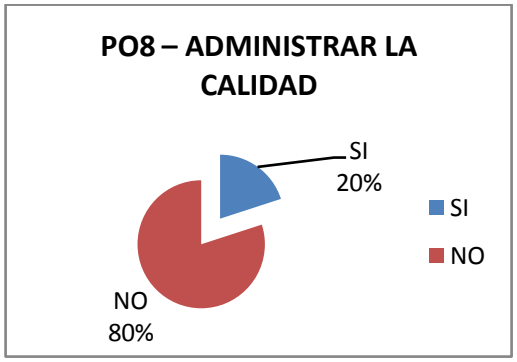

PO3 – DETERMINAR LA DIRECCIÓN TECNOLÓGICA
SI 40%
NO 60%
SI
NO

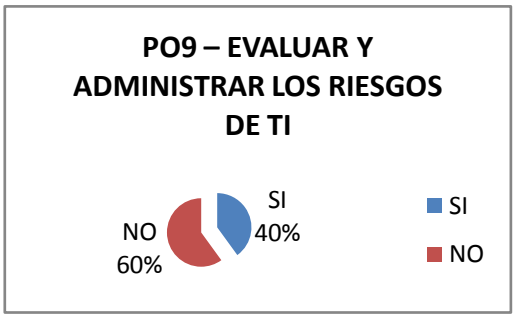

PO4 – DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI
SI 40%
NO 60%
SI
NO

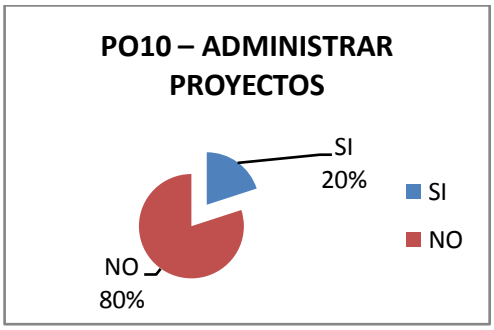

PO5 – ADMINISTRAR LA INVERSIÓN EN TI
SI 0%
NO 100%
SI
NO

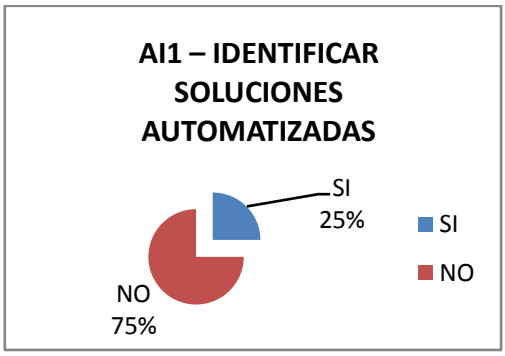

PO6 – COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA…
NO 40%
SI 60%
SI
NO

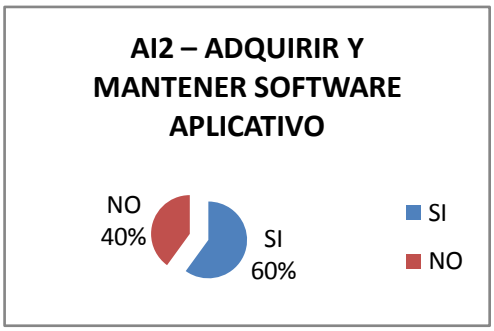

PO7 – ADMINISTRAR RECURSOS HUMANOS DE TI
NO 40%
SI 60%
SI
NO

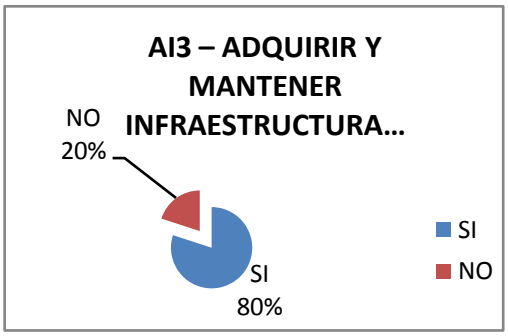

PO8 – ADMINISTRAR LA CALIDAD
SI 20%
NO 80%
SI
NO

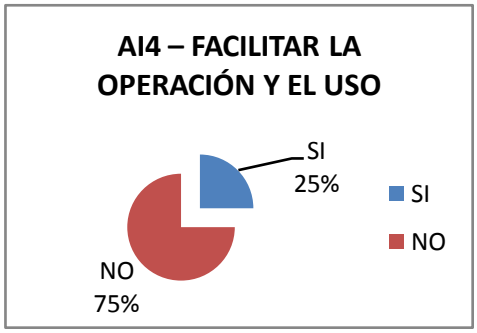

PO9 – EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI
SI 40%
NO 60%
SI
NO

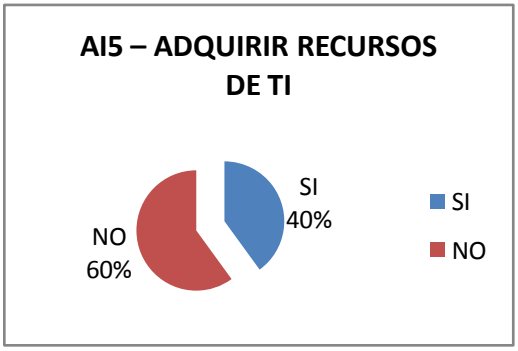

PO10 – ADMINISTRAR PROYECTOS
SI 20%
NO 80%
SI
NO

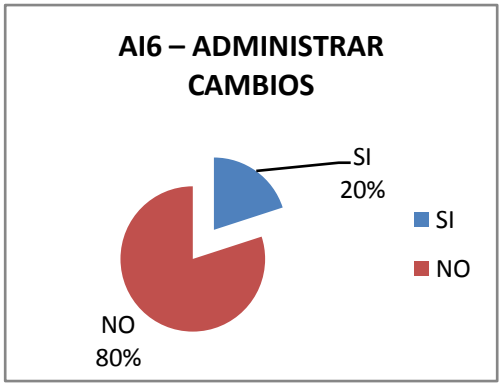

AI1 – IDENTIFICAR SOLUCIONES AUTOMATIZADAS
SI 25%
NO 75%
SI
NO

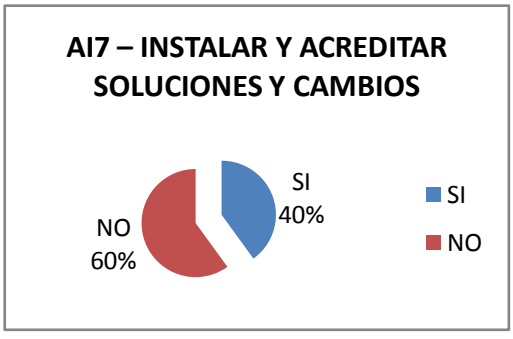

AI2 – ADQUIRIR Y MANTENER SOFTWARE APLICATIVO
NO 40%
SI 60%
SI
NO

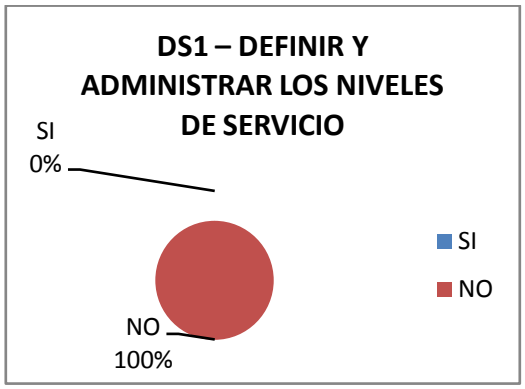

AI3 – ADQUIRIR Y MANTENER INFRAESTRUCTURA…
NO 20%
SI 80%
SI
NO

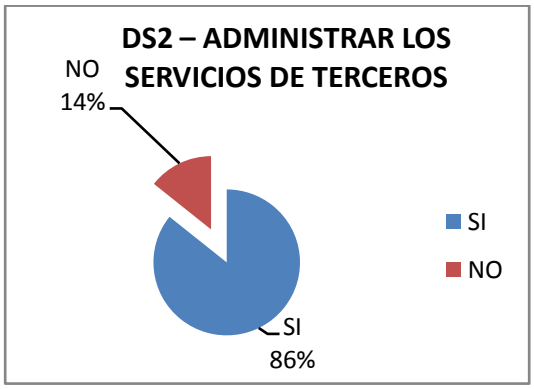

AI4 – FACILITAR LA OPERACIÓN Y EL USO
SI 25%
NO 75%
SI
NO

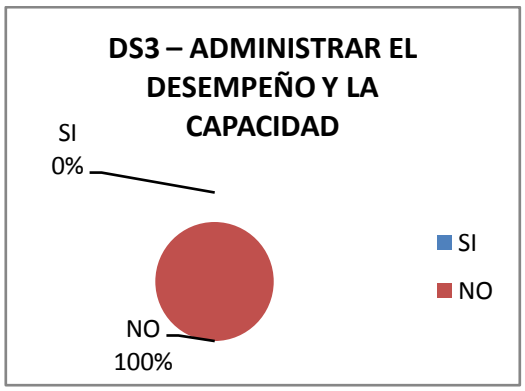

AI5 – ADQUIRIR RECURSOS DE TI
SI 40%
NO 60%
SI
NO

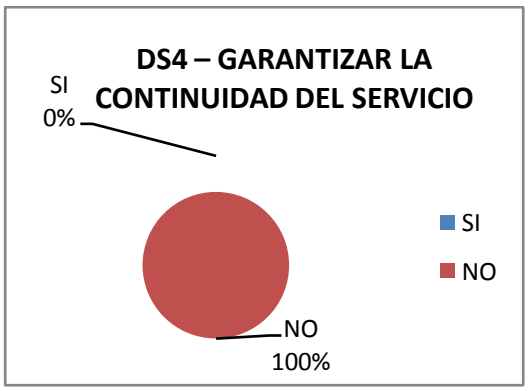

AI6 – ADMINISTRAR CAMBIOS
SI 20%
NO 80%
SI
NO

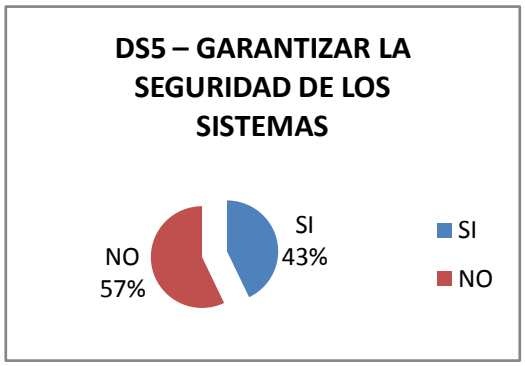

AI7 – INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS
SI 40%
NO 60%
SI
NO

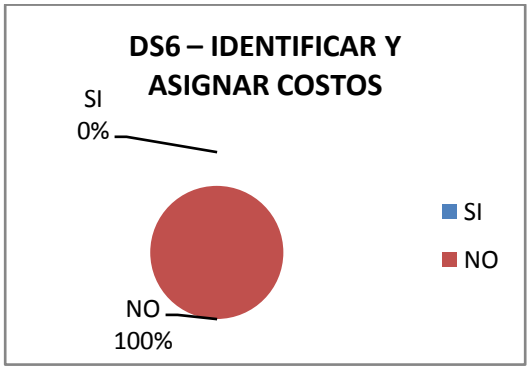

DS1 – DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO
SI 0%
NO 100%
SI
NO

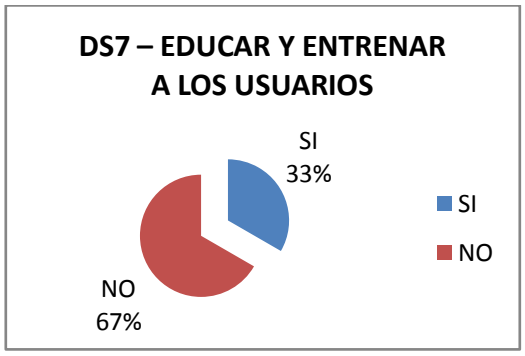

DS2 – ADMINISTRAR LOS SERVICIOS DE TERCEROS
NO 14%
SI 86%
SI
NO

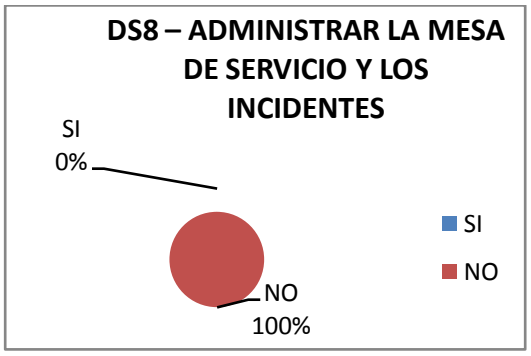

DS3 – ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD
SI 0%
NO 100%
SI
NO

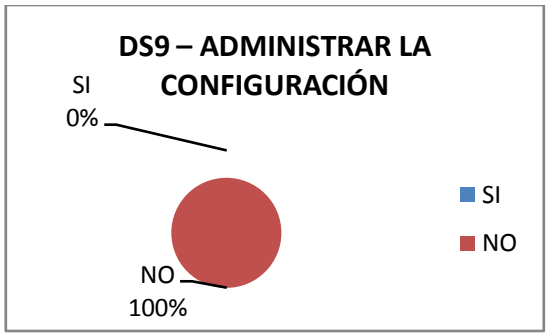

DS4 – GARANTIZAR LA CONTINUIDAD DEL SERVICIO
SI 0%
NO 100%
SI
NO

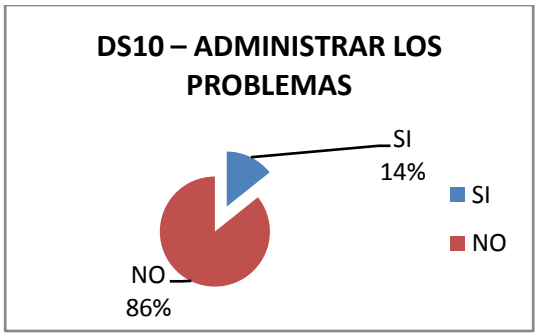

DS5 – GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS
SI 43%
NO 57%
SI
NO

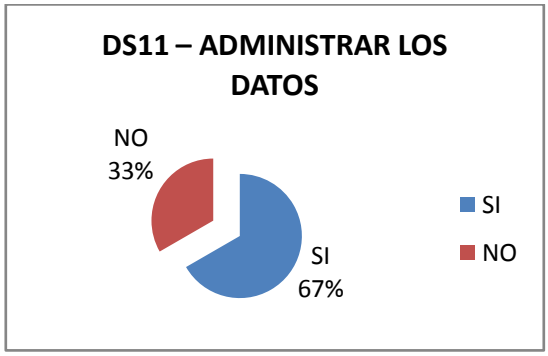

DS6 – IDENTIFICAR Y ASIGNAR COSTOS
SI 0%
NO 100%
SI
NO

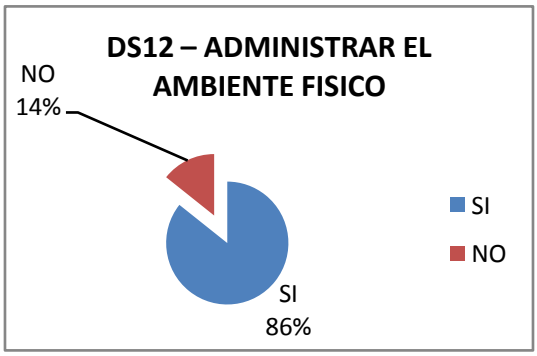

DS7 – EDUCAR Y ENTRENAR A LOS USUARIOS
SI 33%
NO 67%
SI
NO

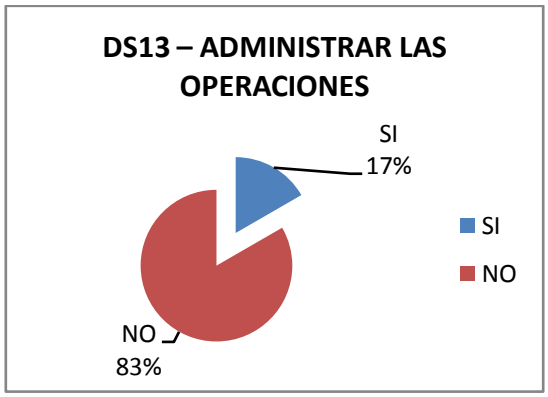

DS8 – ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES
SI 0%
NO 100%
SI
NO

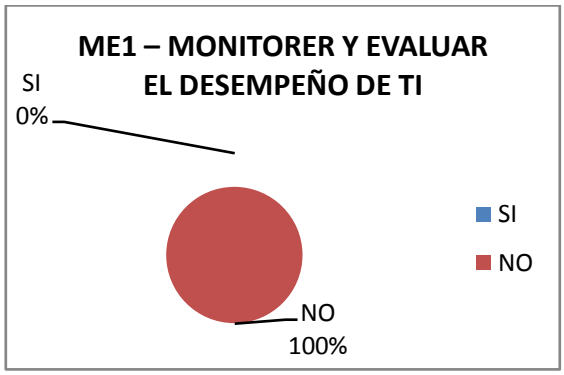

DS9 – ADMINISTRAR LA CONFIGURACIÓN
SI 0%
NO 100%
SI
NO

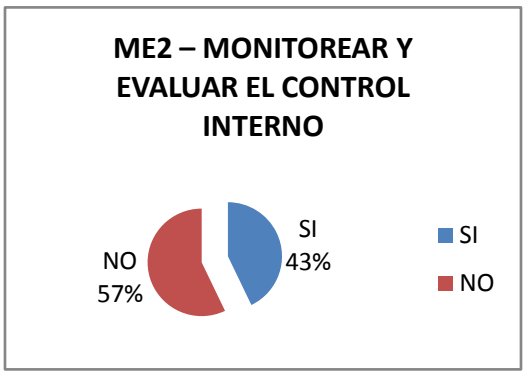

DS10 – ADMINISTRAR LOS PROBLEMAS
SI 14%
NO 86%
SI
NO

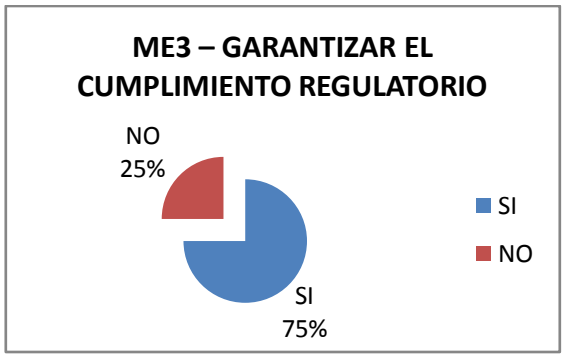

DS11 – ADMINISTRAR LOS DATOS
NO 33%
SI 67%
SI
NO


DS12 – ADMINISTRAR EL AMBIENTE FISICO
NO 14%
SI 86%
SI
NO


DS13 – ADMINISTRAR LAS OPERACIONES
SI 17%
NO 83%
SI
NO


ME1 – MONITORER Y EVALUAR EL DESEMPEÑO DE TI
SI
0%
NO
100%
SI
NO


ME2 – MONITOREAR Y EVALUAR EL CONTROL INTERNO
NO
57%
SI
43%
SI
NO


ME3 – GARANTIZAR EL CUMPLIMIENTO REGULATORIO
NO
25%
SI
75%
SI
NO

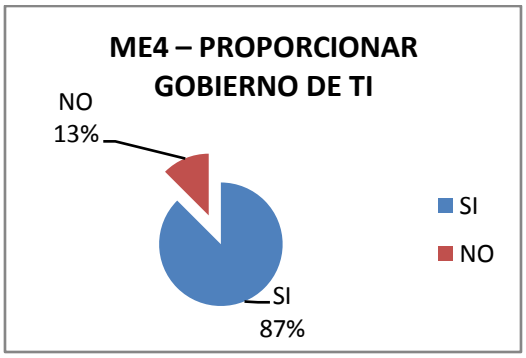
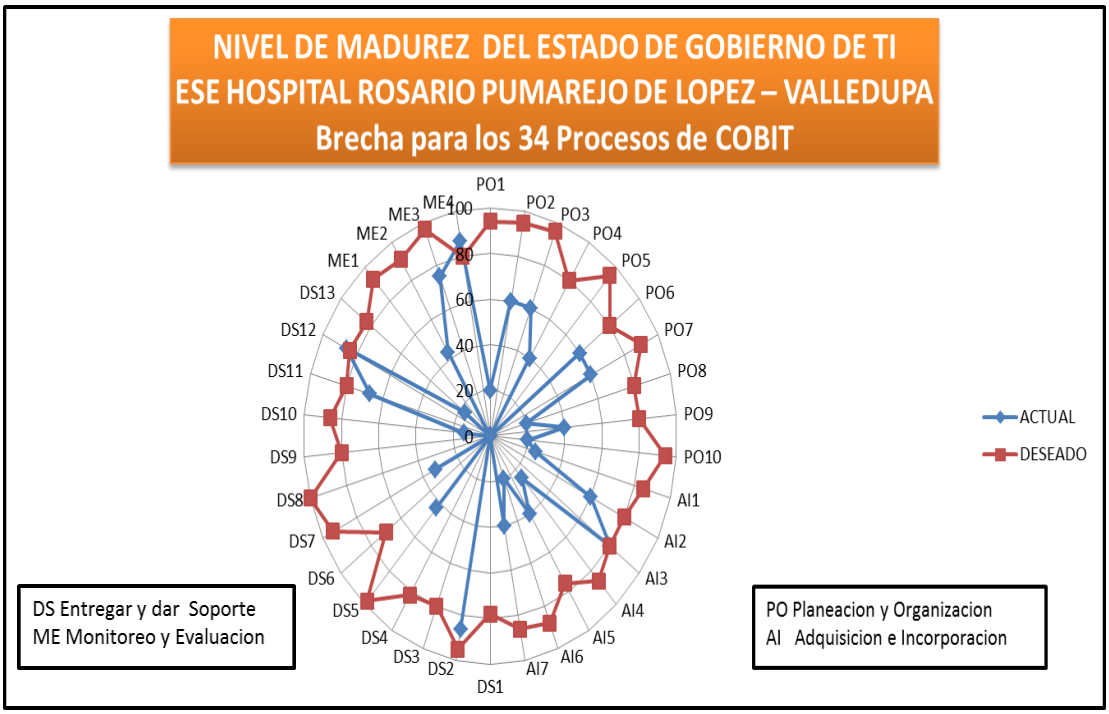

ME4 – PROPORCIONAR GOBIERNO DE TI
NO
13%
SI
87%
SI
NO

FIGURA 6. NINEL DE MADUREZ DEL ESTADO DE GOBIERNO DE TI ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ - VALLEDUPAR



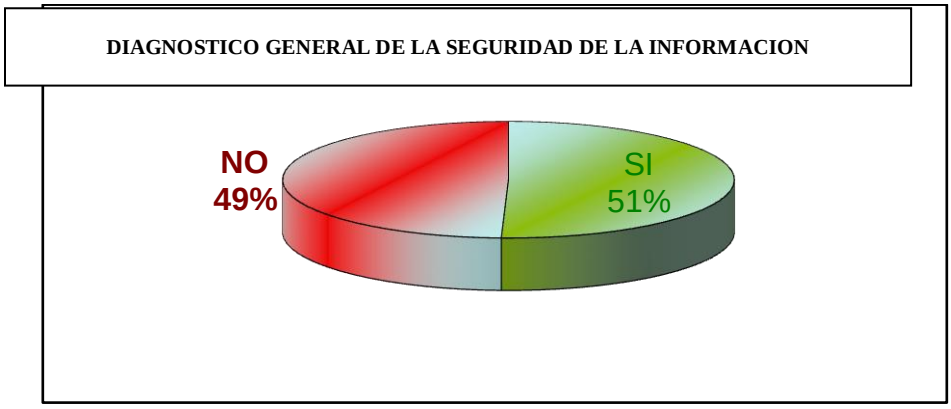
Fuente: el Autor

8.2 Diagnostico de la Seguridad de la Información (ISO/IEC - 27001, ISO/IEC – 27002)

Para el planteamiento del siguiente diagnostico se aplico una la lista de chequeo basada a los precitados estándares, con el objeto de evaluar la Seguridad de la Información en la ESE Hospital Rosario Pumarejo de López.

La Información se tomo de la entrevista aplicada el 6 de julio de 2011 según lista de chequeo, al Ingeniero Gustavo Ariza, funcionario de Cooprosad, Contratista de la ESE y quien actualmente es el encargado de la Administración y Gestión Tecnológica del Call Center. Ver lista de Chequeo en Anexos.

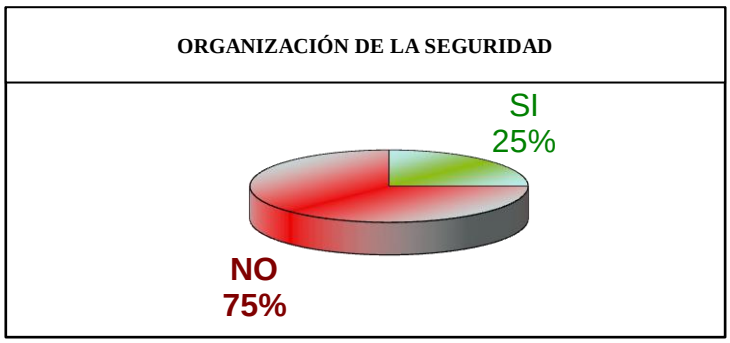
Los siguientes son los resultados, expresados en la siguientes graficas:



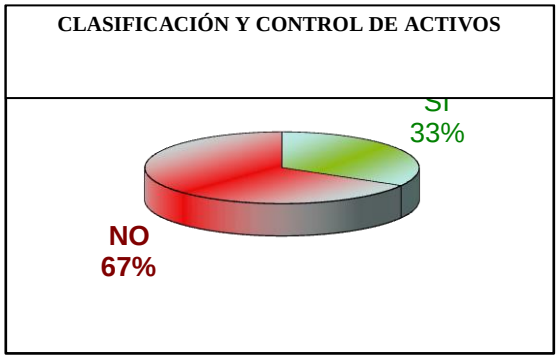
Detalles de este resultado en el punto 1.2.1 Diagnostico por dominio.

DIAGNOSTICO POR DOMINIO

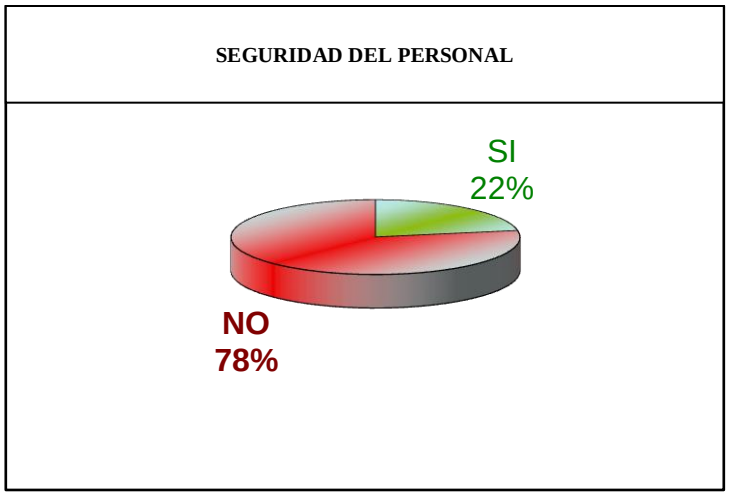
La ESE Cuente con políticas de Información y Comunicación, y Políticas para el uso adecuado de los sistemas de información y computo, pero no se verifica la efectividad y su cumplimiento.



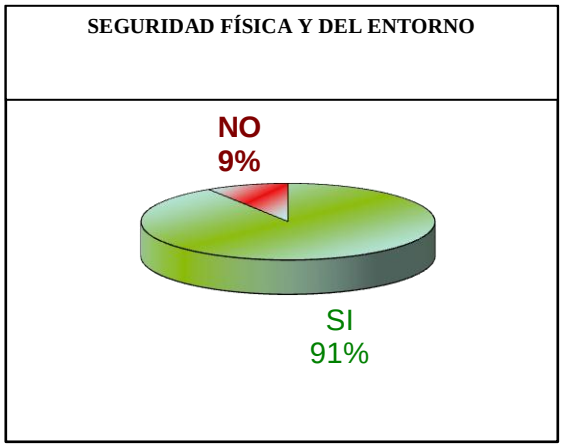
No está organizada la seguridad de la organización, con roles y responsabilidades bien definidos, programas de formación en seguridad para los empleados y no se maneja el tema de acuerdos de confidencialidad en la información que se acceso aunque si es tenido en cuenta para la contratación con terceros.



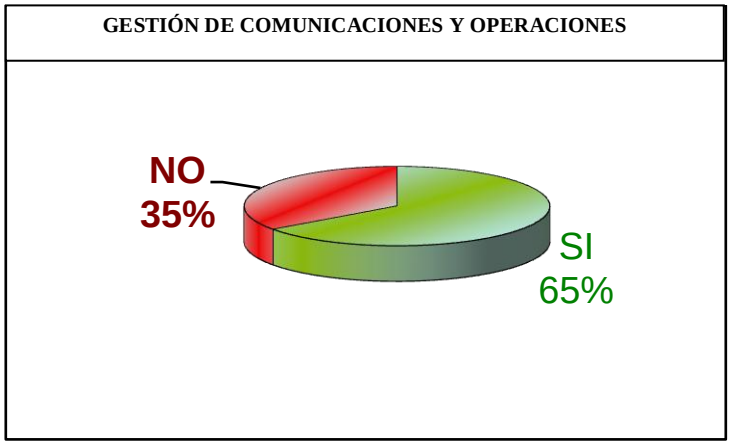
Inadecuada clasificación de activos en la organización, solo se tiene en cuenta el hardware, es decir no hay una clasificación de activos de datos, aplicaciones, servicios. Soporte de aplicación, etc., y se carece de un procedimiento para clasificar la información.



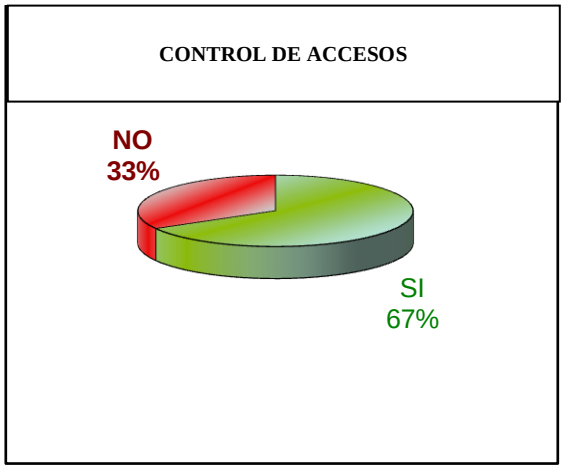
Las políticas de la ESE establecen que cada empleado controla el acceso a información particular almacenada en los sistemas de información, no obstante no se tienen definidos responsabilidades y roles de seguridad, no se imparte adecuada formación en temas de seguridad, y no hay gestión de incidentes de seguridad.



La ESE tiene implementado controles de seguridad física, como el establecimientos de perímetros de seguridad física, cámaras de seguridad en algunas áreas, guardas de seguridad en los acceso a las instalaciones de la ESE y áreas críticas, ambiente adecuados para el funcionamiento de los equipos (acondicionadores de aire), prevención contra las fallas de alimentación eléctrica de red pública (UPS – Sistemas de Alimentación Ininterrumpida, Plan Eléctrica – Generador eléctrico de Respaldo), etc., no obstante se observo que los guardas de seguridad no revisan los bolsos al ingreso y salida de la ESE, además que estos no cuentan con herramientas que le permitan controlar el ingreso de armas e ingreso y salida de vehículos de la ESE.

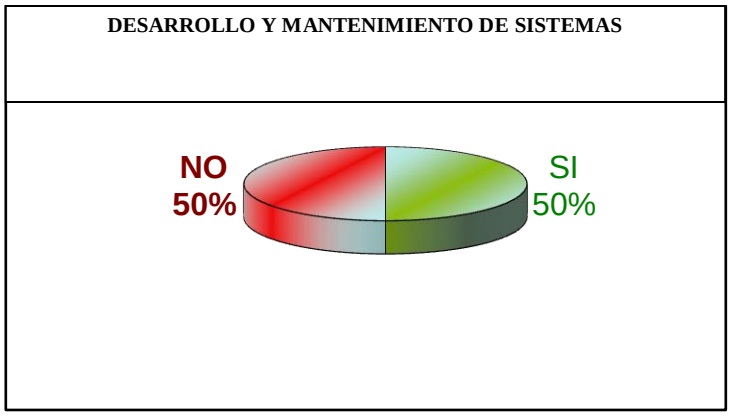


Se observo que no todos los procedimientos operativos identificados en las Políticas, están documentados ni asignadas las responsabilidades para asegurar un respuesta rápida y efectiva frente a incidentes de seguridad, no obstante se observa que existen controles para software maligno, control en las redes, plan de capacidad y existen criterios de aceptación de nuevos sistemas incluyendo nuevas versiones, y se han implementado medidas para proteger la confidencialidad e integridad de información publicada.

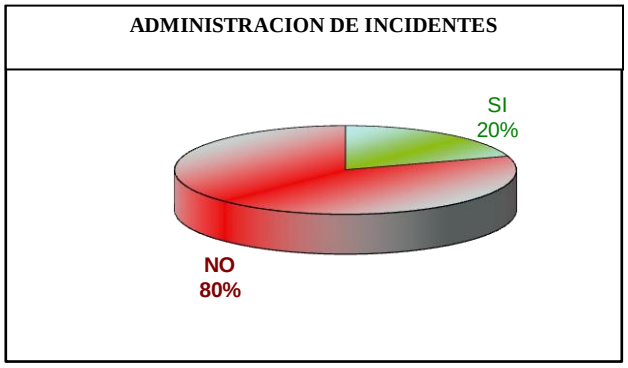


La Entidad cuenta con políticas de control de acceso a los sistemas de información, procedimientos para la asignación de claves y uso de password, y controles de

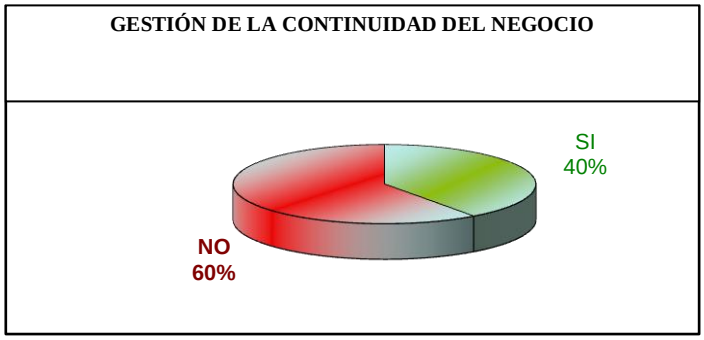
conexión de redes, no obstante no se realiza gestión de los password de los usuarios, ni se revisan los derechos de acceso de los usuarios.



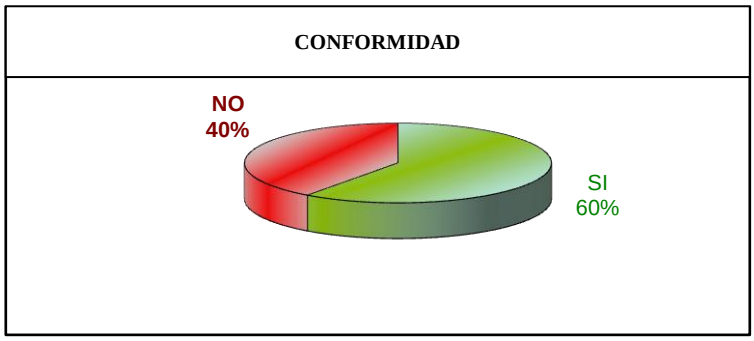
Se asegura que la seguridad está implantada en los sistemas de información, y existen controles de seguridad en los aplicativos (Software Dinámica Gerencial), pero no existe gestión de cambio en los sistemas y no se controlan las vulnerabilidades de los equipos.



Existen responsabilidades asignadas en casos de incidentes de seguridad, pero no se realiza registro ni gestión de los mismos, como tampoco existe un procedimiento formal de respuesta.



Existe un plan de contingencia basado en Backup del área de sistemas para evitar la interrupción de los procesos que esta área soporta (Software Dinámica Gerencial – Soporta los módulos de: Cartera, Contabilidad y Pagos, Presupuesto, Tesorería, Facturación, Activos Fijos, Admisiones y Contratos, Citas Médicas, Hospitalización, Inventarios y Compras) ante fallas de los sistemas por eventos de fuerza mayor, no obstante no existen procesos para la gestión de la continuidad ni se realizan pruebas y reevaluación de los planes de continuidad.



Se tiene en cuenta el cumplimiento de la legislación y regulación por parte de los sistemas, pero no se revisa la política de seguridad.

CAPITULO III

9. ANÁLISIS DEL ÁREA DE TI DE LA ESE HOSPITAL ROSARIO PUMAREJO DE LÓPEZ

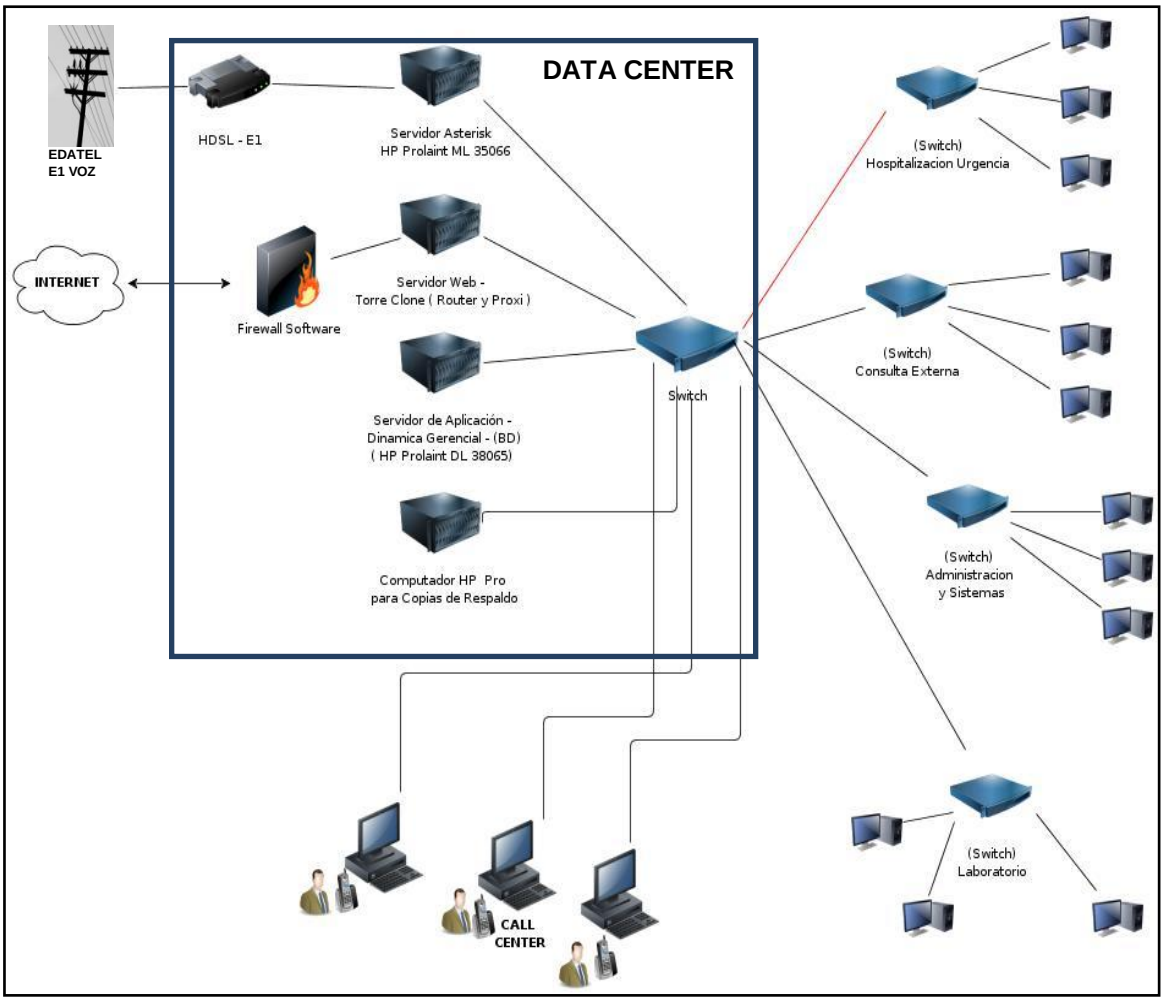
9.1 Recurso Humano

La ESE en su are de sistemas, solo cuenta con Cinco (5) personas, de las cuales solo una tiene vinculación directa con el Hospital, es decir esta nombrada con el cargo de profesional Universitario de Sistemas, y es quien hace la veces de Gerente de TI. El resto de personas lo conforman dos Ingenieros de sistemas cuya vinculación laboral es a través de la cooperativa de trabajo asociado de profesionales administrativos y asistenciales - COOPROSAD que presta servicios de soporte técnico especializado al Hospital Rosario Pumarejo de López desde hace año y medio, y dos aprendices SENA.

Los Ingenieros de Soporte Contratista son quienes administran el Call Center para apartar citas y realmente son los que tienen un conocimiento más profundo en la tecnología implementada para este. Esto representa un riesgo muy alto para la ESE en la medida que se crea una dependencia de estas Cooperativas, por no estar documentadas todas las configuraciones ideales tanto de servidores como de equipos que soportan el Call Center, además que se hace necesario que el área de sistemas tenga por lo menos otro ingeniero de planta y dos técnicos auxiliares, para que el área de T.I. sea más proactiva y menos reactiva, además de un plan de capacitación y entrenamiento del personal no solo en tecnología si no en temas de seguridad que le puedan dar un valor agregado para el proceso de acreditación que busca la ESE.

9.2 Esquema de Infraestructura Tecnológica

La ESE no tiene un esquema de infraestructura tecnológica, por lo que en base al trabajo de campo realizado, se diseño el siguiente:



La Red de la organización es una LAN (Red de Área Local) Fast Ethernet de 100 Mbits construida en una topología Estrella, con un Data Center con todas los requerimientos técnicos y de seguridad para su buen funcionamiento (Piso falso, Acondicionador de aire, Detector de incendios, Extintores, cableado organizado, Racks, controles de

acceso Biométrico, Switchs, etc.) ubicado en las instalaciones administrativas del Hospital, en donde están organizados los servidores (Aplicación, Web, Asterisk – Call Center) y al que acceden los diferentes equipos de computo del hospital a través de la red que los interconecta utilizando switchs en cascadas y cableado estructurado Cat 5 y 6 100 BaseTX además de fibra óptica multimodo 100 BaseFX para enlazar bloques dentro del campus del Hospital.

La red utiliza IP estáticas asignadas por el administrador, pero no está segmentada lo que facilitaría su gestión y mejoraría la seguridad, los equipos de la red utilizan sistemas operativos de Microsoft (Windows Server 2003 en servidor de aplicaciones y Windows 98,XP … 7 en los equipos clientes. En la actualidad hay 238 puntos de red instalados y están siendo usados 120.

9.3 Inventario de Software

De acuerdo a la información suministrada por el área de TI, la ESE tiene un inventario de software, y este está prácticamente licenciado, no obstante no se suministró el inventario para constatar dicha información, aunque en el último inventario suministrado a la Contraloría se observa que hay siete equipos de escritorio que tienen software no licenciado .

Es pertinente la adquisición de las licencias para evitar sanciones a la ESE, y de actualizar las licencias que ya no tienen soporte, el caso de Windows 98.

Los sistemas operativos utilizados en el hospital son:

SISTEMA OPERATIVO	CANTIDAD DE LICENCIAS	INSTALADO EN
Windows Server 2003 Enterprise Edition	1	Servidor de Aplicaciones
SQL Server 2005	1	Servidor de Aplicaciones
Linux Fedora, Ubuntu y Debian	3 (Software libre)	Servidor web y Servidor Asterisk
Windows 98	15	Equipos de escritorio
Windows XP	44	Equipos de escritorio
Windows Vista	30	Equipos de escritorio
Windows 7	31	Equipos de escritorio
TOTAL	125	

Las aplicaciones que se encuentran instaladas en los servidores son:

EQUIPOS	APLICACIONES	ORIGEN DE SOFTWARE
Un Servidor HP Proliant DL380 G5	Dinámica Gerencial Versión 9.0 – Desarrollado en Fox Pro y Base de Datos en SQL Server 2005. – Corre sobre Windows Server 2003 Enterprise Edition.	Sistemas y Asesorías de Colombia (SYAC Ltda)
HP Proliant ML350 G6	Servidor Asterisk (Call Center)	Software Libre bajo Linux que proporciona funcionalidades de una central telefónica.

Equipo Clon	Squid (Proxy)	Proxy Nativo Linux Fedora – Licencia Pública General GNU (**GNU/GPL**).

La Aplicación Dinámica Gerencial (DGH) está desarrollada en Fox Pro con base de datos en SQL Server 2005; DGH es un Sistema Modular Completamente Integrado para el Manejo Médico, Operativo y Financiero para IPS Públicas y Privadas. Consta de más de 35 módulos que integran totalmente el Área Científica con la Facturación y Contabilidad. Es decir, desde el mismo acto médico (Historia Clínica Digital) se afecta en forma automática todo el sistema de información. DGH cumple con todas las normas exigidas por la Ley para el manejo Financiero, Facturación Ley 100 e Historia Clínica. No obstante la aplicación DGH en el Hospital Rosario Pumarejo de López no tiene en funcionamiento el modulo de Historia Clínica y en la actualidad la aplicación esta licenciada pero no cuenta con soporte de la casa desarrolladora SYAC S.A. y la versión utilizada está quedando rezagada de las nuevas versiones que tiene esta aplicación.

9.4 Topología de la Red.

La Red de la organización es una LAN (Red de Área Local) Fast Ethernet de 100 Mbits construida en una topología Estrella.

9.5 Seguridades Físicas.

La ESE Hospital Rosario Pumarejo de López tiene un Data Center implementado en las instalaciones del Hospital, que cumple con todas condiciones de seguridad física y ambientales adecuadas para la conservación de los equipos y el acceso de personal no autorizado, con control biométrico, y cámaras de seguridad.

9.6 Sistema de Respaldo y Protección

La ESE Hospital Rosario Pumarejo de López cuanta con sistema de transferencia automática que cambia el estado de suministro de energía de red pública a planta eléctrica, apoyadas por una fuentes de poder ininterrumpido - UPS.
La ESE cuenta con dos plantas eléctricas de 400 y 320 KVA Marcas CAT y Siemens, las cuales soportan toda la carga del hospital, excepto áreas que no son consideradas como críticas como son lavandería, Cocina, y mantenimiento. Actualmente se está proyectando dejar la Planta Eléctrica Siemens como Soporte de la CAT en caso en que esta falle; a demás el hospital tiene instalado una malla de puestas a Tierras para protección de los equipos Electrónicos.

9.7 Seguridades Lógicas.

Los Sistemas operativos, aplicativos y bases de datos usados en la ESE Hospital Rosario Pumarejo de López, presentan las siguientes debilidades en cuanto a seguridad lógica se refiere:

- La aplicación Dinámica Gerencial Hospitalaria tiene control de acceso a través de cuentas de usuarios que son asignadas por el administrador, con previa autorización de los jefes de área; los sistemas operativos de los servidores tienen control de acceso, pero para las estaciones de trabajo no hay control de acceso a través de password, en su lugar se utiliza una única cuenta para todos, y no se hace revisión de los privilegios asignados a los usuarios.

- El aplicativo Dinámica Gerencial Hospitalaria tiene logs de usuarios, pero no están configurados los logs de ingreso para los usuarios de los sistemas operativos ni de los equipos, o en su defecto no son gestionados, además, no hay una segmentación lógica de la red que permita una mejor administración de los usuarios.

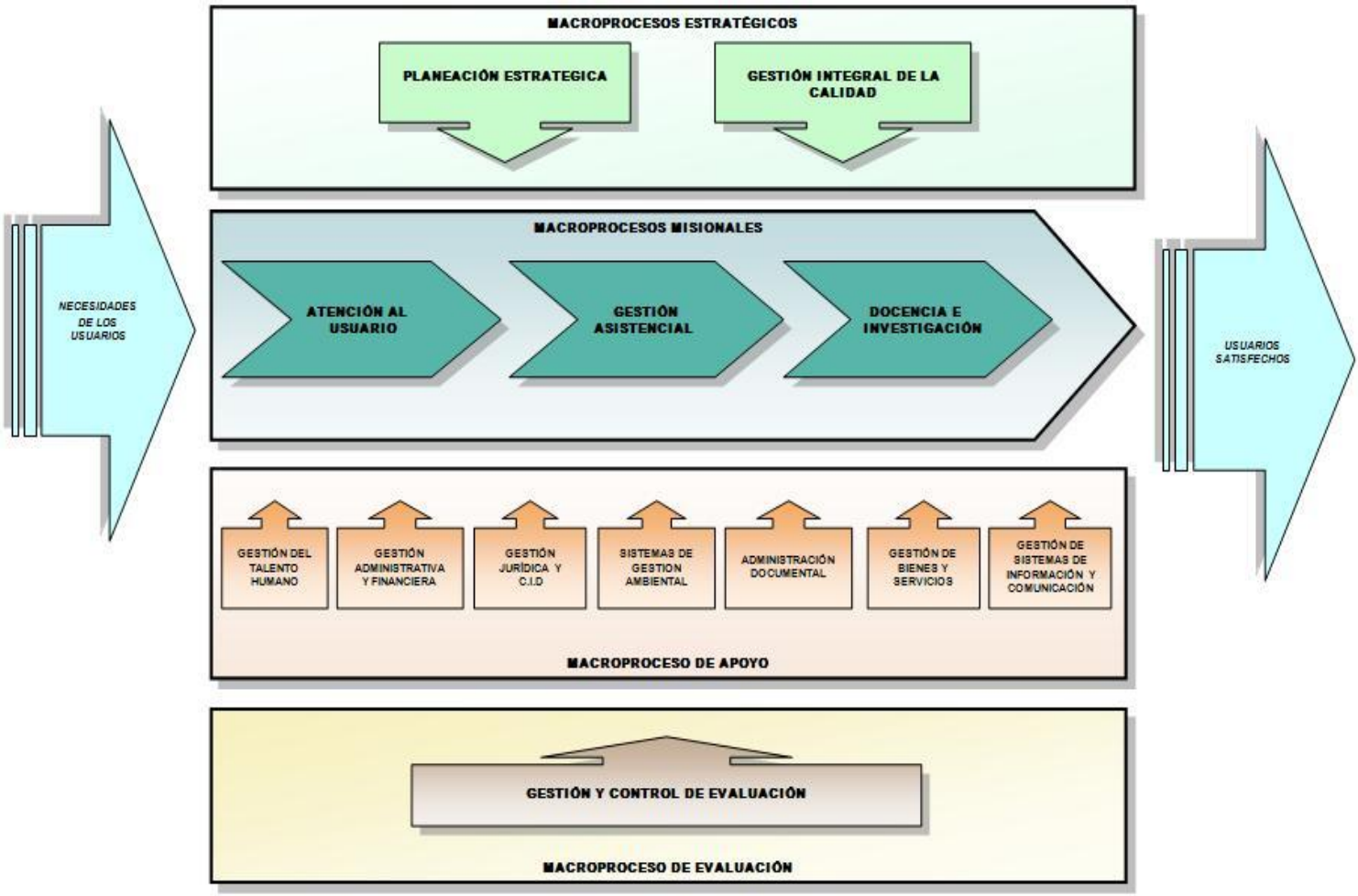
- Los logs del aplicativo Dinámica Gerencial Hospitalaria están protegidos para todos los usuarios excepto para el administrador del aplicativo, igualmente los logs de la Base Datos pueden ser accesados por el DBA, cuya clave es compartida en algunas ocasiones con los demás ingenieros; es decir la clave administrador para Base de Datos, aplicativos y sistemas operativos tiente full control en el sistema y no tiene ningún tipo de restricción. Es importante que se preserve el uso unipersonal de las claves, por esta razón se deberían crear cuentas de usuario con privilegios de administrador para los demás ingenieros, pero con autorización y gestión del Gerente de TI a través de procedimiento formal cuando estos necesiten realizar tareas sobre los aplicativos y/o tablas criticas de las bases de datos. Es también de mucha importancia y para más transparencia de los procesos, que el DBA solo tenga acceso de solo lectura a los Logs, y que control interno tenga una cuenta creada para poder visualizar logs y realizar labores de auditoría.
- El Gerente de TI es quien administra la aplicación Dinámica Gerencial con su respectiva Base de Datos (SQL Server), pero La clave del DBA es compartida en ocasiones con los otros ingenieros de soporte de COOPROSAD. Esta clave cuando es compartida no hay un procedimiento para autorizar su uso, y además cuando se presentan errores en el aplicativo se accede directamente a a la información contenida en la Base de Datos. Es pertinente que cuando se realizan esas actividades por debajo del aplicativo, halla un documento y/o formato que autorice la acción, en este caso el jefe de área que la solicita. Además se debe considerar la realización de scripts cuando estas tareas se vuelvan muy recurrentes.
- Se hace necesario que cuando se realicen acciones en las tablas de la base de datos por fuera de los aplicativos; exista un procedimiento formal para hacerlo, y las tablas críticas en la Base de Datos deberían estar protegidas.

- Actualmente no hay soporte técnico del aplicativo Dinámica Gerencial, lo que se convierte en un riesgo muy alto para la continuidad de las operaciones en la eventualidad en que ocurra un error inesperado en el sistema y no se sepa la causa o en su defecto para la actualización y mantenimiento del mismo software.
- Los archivos y carpetas que pueden tener información relevante no están protegidos, es decir no están definidas ni creadas políticas de protección de estos elementos por el administrador del Windows server, ni por los propietarios de la información.
- La única forma que tienen los usuarios de la red para proteger sus archivos, es guardar la información en la carpeta Mis Documentos que no es compartida, el resto de archivos de los computadores puede ser accedido en la red, ya que no existe segmentación de la red con dominios y cuentas de usuario administradas central mente con políticas y roles de usuario bien definidos en una matriz de roles y perfiles de usuario.
- No está documentada la información de configuración de equipos y servicios que administran y soportan los contratistas de COOPROSAD, lo cual crea una alta dependencia. Se hace necesario garantizar la integridad de las configuraciones de hardware y software, estableciendo un repositorio de configuraciones completo y preciso, disminuyendo la dependencia y aumentando la capacidad de resolución de problemas más rápido.
- El área de TI no lleva un registro de incidentes como tampoco hay bitácoras de solución de los mismos, esto hace los incidentes se vuelvan repetir en el transcurso del tiempo, sin encontrar soluciones rápidas o de fondo.
- La Ese no realiza una adecuada gestión de cambio, en donde haya un procedimiento formal, un plan de pruebas, evaluación de las mismas y puntos de retorno cuando la actualización falle, lo que permita regresar a la versión anterior.
- La ESE Hospital Rosario Pumarejo de López tiene un Data Center implementado en las instalaciones del Hospital, que cumple con todas condiciones de seguridad

física y ambientales adecuadas para la conservación de los equipos, pero de nada sirve que los equipos estén bien protegidos, si ante un daño del servidor de aplicaciones se afecta el funcionamiento del aplicativo Dinámica Gerencial que es quien soporta las demás áreas. En ese orden de ideas se hace necesario la adquisición para funcionamiento redundante, paralelo o espejo de servidor de aplicaciones, servidor web, servidor del Call Center que están importante porque es a través de este sistema que los usuarios pueden apartar citas y la disponibilidad del equipo debe ser prácticamente 24x7.

- La ESE Hospital Rosario Pumarejo de López requiere endurecer mas la seguridad de la Red, por la implementación del Servidor Web y los riesgos que esto representa.

FIGURA 7. MACROPROCESOS ESTRATEGIGOS



Fuente: HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR

CAPITULO IV

10. IDENTIFICACION DE LOS OBJETIVOS DEL PLAN DE GESTION INSTITUCIONAL (PGI) O PLAN ESTRATEGICO CORPORATIVO (PEC) QUE REQUIERAN APOYO TECNOLOGIA INFORMATICA

- Cumplir en el tiempo establecido el reporte de la información del decreto 2193 de 2004.
- Alcanzar la acreditación de la ESE.
- Mejorar la asignación oportuna de citas en consulta médica especializada.
- Cumplir con los estándares para la acreditación.
- Mejorar el porcentaje de satisfacción de los usuarios.

CAPITULO V

11. IDENTIFICACION DE LOS SERVICIOS DE TI ACTUALMENTE OFRECIDOS POR EL AREA DE INFORMATICA

Actualmente el área de TI presta los siguientes servicios en la ESE Hospital Rosario Pumarejo de López.

- Administración de usuarios en la aplicación Dinámica Gerencial.
- Control de acceso a equipos y aplicaciones.
- Control de redes.
- Configuración de equipos servidores.
- Administración de Base de Datos.
- Administración de la Aplicación Dinámica Gerencial
- Administración de centro de datos.
- Administración del Call center para apartar citas.
- Administración y Soporte de Pagina WEB institucional.
- Control de licencias de software.
- Implementación y configuración de equipos y/o software para control de software maligno o intrusos en la redes.
- Soporte Técnico de primer nivel ante fallas en el funcionamiento de equipos y software.
- Disponibilidad de las redes y servidores que soportan la aplicación Dinámica Gerencial.
- Administración de inventario de equipos y de software.

CAPITULO VI

12. DISEÑO DEL PLAN ESTRATÉGICO DE T.I. (PETI), ALINEADO CON LOS OBJETIVOS DEL PLAN DE GESTIÓN INSTITUCIONAL

PLAN DE GESTIÓN INSTITUCIONAL E.S.E. HOSPITAL ROSARIO PUMAREJO DE LÓPEZ, PERIODO 2009 – 2012.

ÁREA	LOGROS A ALCANZAR	ACTIVIDADES GENERALES A DESARROLLAR
GESTIÓN DIRECTIVA Y ESTRATÉGICA	Aumentar el porcentaje de cumplimiento del plan estratégico	Proceso de seguimiento y evaluación que incluya la evaluación de la satisfacción del cliente y partes interesadas
		Seguimiento al Modelo de Operación por Procesos de la ESE que contemple proceso caracterizados (identificación de las interrelaciones, proveedores insumos actividades, clientes, productos, indicadores, normas, entre otros) y adelantar las respectivas evaluaciones en los tiempos fijados por ley.
		Seguimiento Mapa de Procesos y evaluaciones periódicas
	Eliminar el desequilibrio financiero operacional y presupuestal de la ESE	Visita a EPSS y EPS CONTRIBUTIVAS, con el fin de confrontar la facturación radicada y la pagada, para suscribir los respectivos acuerdos de pago de la cartera morosa superior a 60 días
		Suscribir contratos con los intermediarios financieros para marcar las cuentas bancarias como cuentas de recaudo en procura de facilitar la labor de las conciliaciones bancarias y de cartera

ÁREA	LOGROS A ALCANZAR	ACTIVIDADES GENERALES A DESARROLLAR
		Programar visita de conciliación de Glosas generadas por en proceso de facturación por fuera del tiempo estipulado por ley
		Suscribir acuerdo de pago luego de proceso de conciliación de cartera con las distintas EPS
		Implementar proceso de estandarización de verificación de facturación y radicación oportuna de cuentas que deberá evaluarse permanentemente
		Gestión de recaudos con la Gobernación de los giros pendientes
		Realización de Cobros pre jurídicos y jurídicos a las distintas EPS.S
		Conciliaciones de pago con el concurso de Supersalud
		Establecimiento de acuerdos de pagos entre las EPS.S y la E.S.E,
	Aumentar el porcentaje de	Verificación de la facturación y radicación oportuna de cuentas de contratos por venta

	participación de los ingresos provenientes de la venta de servicios de salud en la financiación de la entidad	de servicios
		Diseñar plan de mercadeo para aumento de volumen de servicios ofertados
		Gerencia estratégica de costos para determinar tarifas competitivas
	Mejorar el índice de rotación de cartera.	Diseñar plan de choque para ajustar el índice de rotación de cartera a 60 días.
	Cumplir en el tiempo establecido el reporte de la información del decreto 2193 de 2004	Seguimiento al proceso de registro y validación de la información de los registros en SIHO confrontados con los RIPS
	Elevar la calificación de la gestión del control interno	Seguimiento a la implementación del MECI para cumplir con los estándares exigidos que contribuyan a elevar la calificación a adecuado

ÁREA	LOGROS A ALCANZAR	ACTIVIDADES GENERALES A DESARROLLAR
	Resolver los procesos judiciales en contra (incluidas las tutelas)	Seguimiento y verificación a la Oficina Asesora de Asuntos Jurídicos en la defensa de patrimonio de la ESE frente a los procesos jurídicos en contra
		Establecimiento de registro de procesos judiciales mediante adquisición software que arroje el estado de los mismos y los tiempos de vencimiento de términos
		Exigir reportes quincenales de la acciones cometidas en estas materias para verificar los logros alcanzados
	Alcanzar la acreditación de la ESE	Con la aplicación de los instrumentos señalados en el período de gestión de la actual administración lograr la acreditación
GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE SALUD	Mejorar la asignación oportuna de cita en consulta médica	Adecuar y dotar con tecnología de punta al call center de la ESE
		Redistribuir carga laboral del Coordinador Consulta Externa

	especializada (días)	Ampliar oferta de consultas especializadas de mayor demanda
	Mejorar la atención de urgencias	Mejorar, Ampliar y Dotar las instalaciones Físicas de urgencias
		Implementar plan de capacitación de atención al cliente para humanizar al personal encargado de atención de servicios.
	Disminuir la cancelación de cirugía programada	Brindar capacitación a pacientes sobre recomendaciones y cuidados previos a intervención quirúrgica
		Implementar la valoración pre quirúrgica por anestesiólogo
	Disminuir la proporción de eventos adversos	Garantizar seguridad integral al paciente en la prestación del servicio
		Centrar la atención en el usuario mediante la mejora del servicio personalizado que se otorga

ÁREA	LOGROS A ALCANZAR	ACTIVIDADES GENERALES A DESARROLLAR
	Mejorar el porcentaje de satisfacción de los usuarios	Diseñar e implementar plan de sensibilización y humanización para el paciente
		Centrar la atención en el usuario para lograr que la percepción de satisfacción mejore por el servicio personalizado que se otorga
		Divulgar y masificar el conocimiento del código de ética institucional
	Revisión del cumplimiento de requisitos de habilitación	Solicitar revisión de los cumplimiento de requisitos de habilitación en la periodicidad que exige la normatividad vigente
	Cumplir con los estándares para la acreditación	Seguimiento al proceso de estandarización de procesos para optar a la acreditación
GESTIÓN ADMINISTRATIVA	Pago oportuno de nomina y proveedores	Mejorar los ingresos y recaudos para garantizar el pago de compromiso
	Pago en el término exigido por ley para	Verificar que los funcionarios encargados del pago concepto de

	cumplir con aportes a seguridad social	seguridad social exigidos por ley se cancele en la periodicidad requerida
	Pago oportuno deuda de parafiscales	Verificar el el pago oportuno por concepto de parafiscales exigidos por ley a los responsables de dicha acción
	Mejorar la atención y resolución de los accidentes de trabajo durante el período	Gestionar oportunamente la atención a los accidentes de trabajo identificados.
	Fenecimiento de la cuenta	
	Realizar pago oportuno de los compromisos con contratistas y terceros	Implementar del Plan Anualizado Mensualizado de Caja

CAPITULO VII

13. PLAN ESTRATÉGICO DE T.I. PROPUESTO PARA EL PERIODO 2012.

En base a las actuales condiciones y capacidades de la infraestructura de TI, se hace necesaria la planeación estratégica de TI para gestionar y dirigir todos los recursos de TI en línea con los objetivos del plan de gestión para la consecución de los objetivos del negocio.

El desarrollo del plan Estratégico de TI le permitirá a la alta dirección mejorar la compresión de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identificando la capacidad y los requerimientos de recursos humanos.

Partiendo de los resultados del diagnostico realizado y luego de identificar los objetivos del Plan de Gestión Institucional que requieren apoyo de Tecnología de Información, se propone el siguientes Plan de Estratégico de T.I. para el Periodo 2012, el cual se encuentra alineado con los objetivos del Plan de Gestión.

OBJETIVO GENERAL

Endurecer la infraestructura tecnológica de la E.S.E. Hospital Rosario Pumarejo de López, de tal manera que contribuya al logro de los objetivos del plan de gestión institucional y soporte todos los procesos que apoyen la continuidad de las operaciones del Hospital.

OBJETIVOS ESPECÍFICOS

- Garantizar el funcionamiento ininterrumpido de los servicios críticos ofrecidos por TI y que repercuten en la calidad del servicio prestado al usuario.
- Mejorar la seguridad de la información procesada en la E.S.E Hospital Rosario Pumarejo de López.
- Optimización de la red de datos y del aplicativo Dinámica Gerencial, para la prestación de un mejor servicio tanto al usuario interno como externo.
- Asegurar la disponibilidad, integridad, y confidencialidad de la información como base para el proceso de toma de decisiones de manera oportuna y garantizando la entrega de información pertinente a los diferentes entes regulatorios.

PLAN ESTRATÉGICO DE T.I

No.	PROYECTO	OBJETIVO	JUSTIFICACIÓN
1.	Adquisición y configuración de Servidores redundantes para Servidor de Aplicaciones, Servidor del Call Center y Servidor Web.	Garantizar el funcionamiento ininterrumpido de la aplicación Dinámica gerencial, el Call Center, y la disponibilidad de la	Actualmente en caso de presentarse fallos en el funcionamiento ya sea en el servidor de aplicaciones, servidor del Call Center o el servidor WEB, significa que la aplicación Dinámica Gerencial

		Pagina WEB institucional.	que da soporte prácticamente a todas las áreas queda off-line o en su defecto el usuario no puede apartar citas por caída del Call Center.
2.	Adquisición de servidor para administración de Red.	Organizar lógicamente el funcionamiento de la red, utilizando un servidor especializado para la administración de usuarios, servidor de nombres de dominios entre otros, que permita poder realizar la administración de la red más eficientemente.	Se tiene licencia de Windows Server 2003 Enterprise, pero está siendo subutilizado porque este no se usa para la administración de la red. Además se justifica la adquisición del servidor para administración de la red porque los servicios que hay que montarle para la administración de usuarios y segmentación de la red en dominios recargarían el servidor en donde corre la aplicación Dinámica Gerencial.
3.	Soporte al sistema Dinámica Gerencial	Garantizar el soporte Técnico y Actualización de la aplicación Dinámica Gerencial.	En este momento la aplicación Dinámica Gerencial no tiene soporte de la casa desarrolladora SYAC S.A.; y la versión utilizada está quedando rezagada de las nuevas versiones que tiene esta aplicación. Esto hace que la aplicación no se le este sacando el mayor provecho, por desconocimiento de todas las

			potencialidades de esta, como también el no tener acceso a las actualizaciones realizadas al software para corregir fallas detectadas.
4.	Poner en funcionamiento el modulo Historia clínica en la aplicación Dinámica Gerencial.	Disminuir tiempos de respuesta en consultas, organización de la información y facilitar el acceso a la historia clínica de los usuarios, permitiendo la prestación de un mejor servicio a los mismos.	En la actualidad el proceso de realización y consulta de las historias clínicas se realiza en forma manual, afectando la calidad del servicio prestado al usuario por la cantidad de información que se maneja, incrementando los tiempos de repuesta y la criticidad de la misma.
5.	Capacitación y Entrenamiento del personal de TI en temas de seguridad, Administración de redes Server, y Sistemas de Gestión de Seguridad de la Información.	Mejorar las competencias y potencialidades de los funcionarios del área de sistemas, que le permitan realizar una adecuada administración de la red y controlar las debilidades en temas de seguridad de la información.	En la actualidad no se realiza una adecuada administración de usuarios en la red, no hay una matriz de roles y perfiles de usuario para el control de acceso al sistema operativo y Dinámica Gerencial, no hay segmentación lógica de la red en dominios, como tampoco están contemplados los temas de protección de ficheros y carpetas para usuario.
6.	Implementar un sistema	Realizar la	Se encontraron muchas

	de gestión de seguridad de la información.	implementación de un Sistema de Gestión de Seguridad de la información, que le permita a la organización establecer controles de seguridad en todos los recursos computacionales mejorando la fiabilidad en la seguridad de la información, generándole un valor agregado en el proceso de acreditación de la E.S.E.	debilidades en temas como: - Gestión de archivos logs. - Gestión de usuarios. - Ausencia de procedimientos formales para realizar acciones en la base de datos por debajo de la aplicación. - Uso compartido de claves de administrador de Base de Datos. - Ausencia de procedimientos de gestión de cambios. - Administración de la configuración por ausencia de repositorio de configuraciones de hardware y software. - Control de acceso al sistema operativo. - Ausencia de registros de incidentes. - Entre otras.
7.	Optimización del funcionamiento de la red LAN	Optimizar y mejorar el funcionamiento y seguridad de la red LAN en el campus del hospital, con la asesoría de expertos	La red no está segmentada y los controles de seguridad implementados no son suficientes o ideales para una red LAN que tiene servidor web.

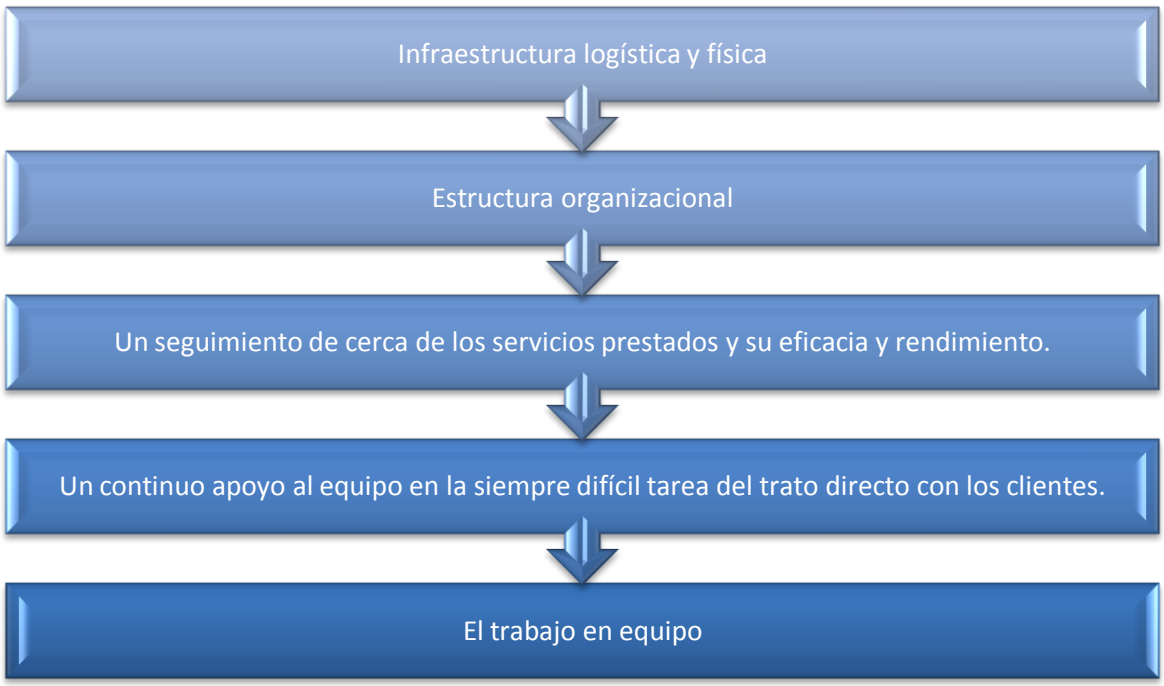
		en el Tema, que permita una adecuada segmentación de la Red, Con los equipos activos de red Necesarios para garantizar su correcto funcionamiento (uso de Switch capa 3, router y configuración de un firewall Screend Host Firewall, etc)	
8.	Adquisición de Licencias de software	Tener todo el software que se usa en el hospital completamente licenciado, para darle cumplimiento a las leyes de derecho de autor y propiedad intelectual.	Se encontró software no licenciado instalado en los equipos del Hospital.
9.	Mantenimiento de los equipos y redes de datos.	Asegurar el buen funcionamiento y la vida útil de los equipos.	Se hace necesario continuar realizando los mantenimientos preventivos y/o correctivos que permiten detectar fallas de manera oportuna, minimizando la posibilidad de pérdida de información o traumatismo en

			los proceso.
10.	Evaluación y adquisición de software antimalware.	Evaluar periódicamente en paginas oficiales el comportamiento, efectividad y actualización de base de firma de virus de los diferentes antimalware del mercado para adquirir el de mejor comportamiento.	Se puede presentar lentitud en el funcionamiento de los equipos, o en el peor de los casos perdida de la disponibilidad de la información por una base datos de antivirus no actualizada.
11	Instalación y operación del servicio de mesa de ayuda o Help Desk	Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de T.I.	Actualmente no hay registro de incidentes y la solución de los problemas tecnológicos no es oportuna porque no se hace un escalamiento adecuado del incidente ni análisis de tendencia y de resolución, lo que mejoraría los tiempos de repuesta.

CAPITULO VIII

14. IDENTIFICACIÓN DE NUEVOS SERVICIOS DE TI DERIVADOS DE IMPLEMENTAR PETI.

Procesos para la gestión de servicios de TI



No.	SERVICIOS	IDENTIFICACION DE LOS SERVICIOS	ACTIVIDADES GENERALES A DESARROLLAR
1.	Instalación y operación del servicio de Mesa de Ayuda.	Para que el área de T.I. sea más proactiva y menos reactiva, además de un plan de capacitación y entrenamiento del personal no solo en tecnología si no en temas de seguridad que le puedan dar un valor agregado para el proceso de acreditación que busca la ESE.	El área de sistemas tiene que tener por lo menos otro ingeniero de sistemas de planta y dos técnicos auxiliares,
2.	Gestión de usuarios	La Entidad cuenta con políticas de acceso a los sistemas de información, procedimientos para la asignación de claves y uso de password, y controles de conexión de redes, no obstante no se realiza gestión de los password de los	Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

		usuarios ni se revisan los derechos de acceso de los usuarios.	
3.	Registro de Incidentes	Existen responsabilidades asignadas en casos de incidentes de seguridad, pero no se realiza gestión de los mismos ni existe un procedimiento formal de respuesta.	Se debe establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización. Y se desarrollan contactos con especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, monitorear los estándares y evaluar los métodos y proporcionar vínculos adecuados para el Manejo de los incidentes de seguridad de la información.
4.	Gestión de activos.	Inadecuada clasificación de activos en la organización, solo se tiene en cuenta el hardware, es decir no hay una clasificación de activos de datos, aplicaciones,	Todos los activos debieran ser inventariados y contar con un propietario nombrado.

		servicios. Soporte de aplicación, etc., y se carece de un procedimiento para clasificar la información.	
5.	Gestión de las operaciones y las comunicaciones	Se observó que no todos los procedimientos operativos identificados en las Políticas, están documentados ni asignadas las responsabilidades para asegurar un respuesta rápida y efectiva frente a incidentes de seguridad	Se deben establecer las responsabilidades y procedimientos para la gestión y operación De todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiado
6.	Planeación y aceptación del sistema	Existe un plan de contingencia del área de sistemas para evitar la discontinuidad de los procesos que esta área soporta (Software Dinámica Gerencial – Soporta Cartera, Contabilidad Y Pagos,	planeación y preparación anticipadas para asegurar la disponibilidad de la Capacidad y los recursos adecuados para entregar el desempeño del sistema requerido. Se debe monitorear, afinar el uso de los recursos y se debe realizar proyecciones de los Requerimientos de capacidad

		Presupuesto, Tesorería, Facturación, Activos Fijos, Admisiones Y Contratos, Citas Médicas, Hospitalización, Historia Clínica E Inventarios Y Compras) ante fallas de los sistemas o eventos de fuerza mayor o siniestros que afecten la operación de los mismos, no obstante no existen procesos para la gestión de la continuidad ni se realizan pruebas y reevaluación de los planes de continuidad.	futura para asegurar el desempeño requerido del sistema.
7.	Gestión de seguridad de redes.	No está organizada la seguridad de la organización, con roles y responsabilidades bien definidos, programas de	Se debieran establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la

		formación en seguridad para los empleados y no se maneja el tema de acuerdos de confidencialidad en la información que se acceso	Información.

15. CONCLUSIONES Y RECOMENDACIONES

15.1 Conclusiones

Los Objetivos de Control para la Información y la Tecnología relacionada **(COBIT),** representa el mejor estándar a nivel mundial para el gobierno de TI, Este modelo esta enfocado fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implantar un sistema de control interno o un marco de trabajo. Se observa que las entidades de salud no han implementado un marco de referencia para la planificación y organización de la infraestructura tecnológica que deben soportan cada uno de sus procesos.

El Modelo Cobit, las normas ISO 27001, 27002, 20000 e ITIL representan las mejores prácticas, para su implementación en las organizaciones y la articulación de cada una de ellas conforman un modelo guía útil para una adecuada planificación de TI, para las entidades de salud como la ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLDUPAR brindara una oportunidad de alinear las estrategias de TI con las estrategias del hospital, de alcanzar el uso optimo de todos sus recursos que ayudaran a satisfacer las necesidades de la entidad y los requisitos de los usuarios, Cumplir con la legislación, prestar un mejor servicio, revisarse y mejorarse de forma continua. Con la implementación de estos estándares contribuirá a proporcionar una base de control de TI en las entidades de salud.

15.2 Recomendaciones

Es imperativo el apoyo irrestricto de la Gerencia de la ESE Hospital Rosario Pumarejo de López, para la implementación y puesta en marcha del Plan Estratégico de TI como único camino trazado y proactivo, para el soporte y logro de los objetivos planteados en el Plan de Gestión Institucional.

La oficina de Control Interno en conjunto con el equipo MECI, deben focalizar como tema importante dentro de sus actividades, el componente de auditoría a los sistemas de Información de una manera profunda y objetiva que garantice la seguridad y el control de los Procesos de TI.

Ampliar el número de funcionarios con cargos creados en el área de Tecnología Informática, para minimizar los riesgos que representa tener procesos o servicios tercerizados cuando la criticidad de estos es muy alta.

REFERENCIAS BIBLIOGRÁFICAS

- Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa, IT Governance Institute, Isaca (2008).

- AS/NZ 4360. Guía para la administración del riesgo.

- COBIT 4.1. ISACA. Marco de Trabajo, Objetivos de Control, Directrices Gerenciales y Modelos de Madurez.

- COBIT Control Practices. ISACA. Guidance to Achieve Control Objetives for Succesful IT Governance.

- Cristrian Bailey. ITIL V. 3. Manual Técnico.

- CMMI. Manual de Referencia.

- Cubillos Gordillos,Amilkar; Garcia Munive, Javier, "ELABORACION DEL PLAN ESTRATEGICO EN SISTEMAS DE LA SECRETARIA DE CONTROL URBANO Y ESPACIOPUBLICO DE LA ALCALDIA DISTRITAL DE BARRANQUILLA", Corporación Universitaria de la Costa, Especialización en Auditoria de Sistemas de Información, Barranquilla, 2010.

- (ERICKSON, 1986); Citado por: Documento PEÑA, Judith, Naturaleza de la Investigación, p 40 - 41.

- Gobierno de TI - TCP Sistemas e Ingeniería, http://www.tcpsi.com/servicios/gobierno_ti.htm

- Introducción ISO20000 COLOMBIA, http://www.iso20000.com.ar/intro_col.html

- IT Assurance Guide. Using COBIT. ISACA. (2007)
- IT Governance Institute, Cobit 4.1 – Isaca (2010).
- ISO/IEC 27001, http://es.wikipedia.org/wiki/ISO/IEC_27001

- ISO 27001 e ISO 27002. Manual de Referencia.

- Martinez del Vecchio, Zeudy Carroll, " PROPUESTA DE UN MARCO DE REFERENCIA PARA LA PLANEACION Y ORGANIZACIÓN DE LAS T.I.C. BASADO EN COBIT QUICK START, EN EL COLEGIO DE LA COMPAÑÍA DE MARIA LA ENSEÑANZA BARRANQUILLA", Corporación Universitaria de la Costa, Especialización en Auditoria de Sistemas de Información, Barranquilla, 2010.

- Sitio en Internet, Disponible en :
  HTTP://HRPLOPEZ.GOV.CO/HOSPITAL/INDEX.PHP?OPTION=COM_FRONTPAGE&ITEMID=1

- Sitio en Internet, Disponible en:
  http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php.

- Sitio en Internet, Disponible en:
  http://www.es.sgs.com/es/iso_20000?serviceId=10009985&lobId=1998.

- Sitio en internet, Disponible en:
  http://www.virtual.unal.edu.co/cursos/agronomia/2008868/lecciones/capitulo_2/cap2lecc2.htm.

- Sitio en Internet, Disponible en: http://www.deloitte.com/view/es_PE/pe/servicios/consultoria/tecnologia-de-la-informacion/gobierno-de-ti/index.htm.

ANEXOS

Anexo 1 LISTA DE CHEQUEO PARA DIAGNOSTICO COBIT

PO → PLANEAR Y ORGANIZAR			
PO1 – DEFINIR UN PLAN ESTRATÉGICO DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La gerencia de TI conoce la necesidad de una planeación estratégica de TI alineada con los objetivos corporativos?		
2	¿La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo?		
3	¿Existen procesos bien definidos para determinar el uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas?		
4	¿Las consideraciones de riesgo y de valor agregado se actualizan de modo constante en el proceso de planeación estratégica de TI?		
5	¿Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia?		
PO2 – DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia de la importancia de la arquitectura de la información?		
2	¿La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara?		
3	¿Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas		

	formales?		
4	¿El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio?		
5	¿Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua?		
PO3 – DETERMINAR LA DIRECCIÓN TECNOLÓGICA			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad?		
2	¿Existe un plan de infraestructura tecnológica definido, documentado y bien difundido?		
3	¿La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica han sido asignados?		
4	¿Se han incluido buenas prácticas internas en el proceso?		
5	¿Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales?		
PO4 – DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen roles y responsabilidades definidos para la organización de TI y para terceros?		
2	¿La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI y se define el ambiente de control interno?		
3	¿La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas?		
4	¿La gerencia de TI cuenta con la experiencia y habilidades		

	apropiadas para definir, implantar y monitorear la organización deseada y las relaciones?		
5	¿Se ponen en funcionamiento las mejores prácticas de la industria y existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI?		
PO5 – ADMINISTRAR LA INVERSIÓN EN TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un entendimiento de la necesidad de seleccionar y presupuestar y comunicar las inversiones?		
2	¿Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología?		
3	¿El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio?		
4	¿Se utilizan las mejores prácticas de la industria para evaluar los costos por comparación e identificar la efectividad de las inversiones?		
5	¿Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión?		
PO6 – COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La gerencia es reactiva al resolver los requerimientos del ambiente de control de información?		
2	¿La gerencia tiene un entendimiento de las necesidades y de los requerimientos de un ambiente de control de información efectivo?		
3	¿El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal?		
4	¿El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora?		
5	¿Se asignan expertos internos y externos para garantizar que se		

	adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación?		
PO7 – ADMINISTRAR RECURSOS HUMANOS DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia sobre la importancia de alinear la administración de recursos humanos de TI con el proceso de planeación de la tecnología para la organización?		
2	¿El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal?		
3	¿Existe un proceso definido y documentado para administrar los recursos humanos y un enfoque estratégico para la contratación y la administración del personal de TI?		
4	¿La organización cuenta con métricas estandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de TI?		
5	¿Los componentes de la administración de recursos humanos de TI son consistentes con las mejores prácticas de la industria, tales como compensación, revisiones de desempeño, participación en foros de la industria, transferencia de conocimiento, entrenamiento y adiestramiento?		
PO8 – ADMINISTRAR LA CALIDAD			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La alta dirección y el equipo de TI no reconocen que un programa de calidad es necesario?		
2	¿Se establece un programa para definir y monitorear las actividades de QMS dentro de TI?		
3	¿Se usan métodos de análisis de costo/beneficio para justificar las iniciativas de QMS?		
4	¿Los procesos de QMS son flexibles y adaptables a los cambios en el ambiente de TI y mejora la base de conocimientos para métricas de		

	calidad con las mejores prácticas externas?		
5	¿Se realiza benchmarking contra estándares externos rutinariamente?		
PO9 – EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se realiza la evaluación de riesgos para los procesos y las decisiones de negocio?		
2	¿Se tienen en cuenta los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad proyecto por proyecto?		
3	¿La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados?		
4	¿La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI?		
5	¿La dirección evalúa las estrategias de mitigación de riesgos de manera continua?		
PO10 – ADMINISTRAR PROYECTOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos?		
2	¿El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados?		
3	¿Se han establecido los criterios para evaluar el éxito en cada punto clave?		
4	¿El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos?		
5	¿La planeación de programas y proyectos en toda la organización garantiza que los recursos de TI y del usuario se utilizan de la mejor manera para apoyar las iniciativas estratégicas?		
AI → ADQUIRIR E IMPLEMENTAR			
AI1 – IDENTIFICAR SOLUCIONES AUTOMATIZADAS			

N°	PREGUNTA	SI	NO
1	¿Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas?		
2	¿Existe una metodología clara para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos?		
3	¿Existe interfaz definida de forma clara entre la gerencia de TI y la del negocio para la identificación y evaluación de las soluciones de TI?		
4	¿Se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general?		
AI2 – ADQUIRIR Y MANTENER SOFTWARE APLICATIVO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones?		
2	¿Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo?		
3	¿Las actividades de mantenimiento se planean, programan y coordinan?		
4	¿Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación?		
5	¿Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones?		
AI3 – ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto?		
2	¿Existe un claro, definido proceso para adquirir y dar mantenimiento a		

	la infraestructura TI?		
3	¿El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología?		
4	¿Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración?		
5	¿Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización?		
AI4 – FACILITAR LA OPERACIÓN Y EL USO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre?		
2	¿Se utilizan herramientas automatizadas en la generación y distribución de procedimientos?		
3	¿Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI?		
4	¿El desarrollo de materiales de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones de proceso del negocio?		
AI5 – ADQUIRIR RECURSOS DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso definido de adquisición de recursos de TI?		
2	¿La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización?		
3	¿Se determinan responsabilidades y rendición de cuentas para la		

	administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato?		
4	¿Existen estándares de TI para la adquisición de recursos de TI y los proveedores de recursos de TI?		
5	¿La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI?		
AI6 – ADMINISTRAR CAMBIOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y de los beneficios de la buena administración de cambio?		
2	¿Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio?		
3	¿Se da un proceso de aprobación para cambios?		
4	¿Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios?		
5	¿El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas?		
AI7 – INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe consistencia entre los enfoques de prueba y acreditación?		
2	¿Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados?		
3	¿El sistema de prueba refleja adecuadamente el ambiente de producción?		
4	¿Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente		

	de entrenamiento, pruebas y transición a producción para los nuevos sistemas?		
5	¿Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción?		
DS → ENTREGAR Y DAR SOPORTE			
DS1 – DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso que defina y administre los niveles de servicio del departamento de TI?		
2	¿Se han asignado responsables de la administración de los niveles de servicios?		
3	¿El proceso de administración de los niveles de servicios ha sido comunicado a la organización?		
4	¿Los servicios y niveles de servicio se encuentran documentados?		
5	¿Qué herramientas son utilizadas para la administración de los niveles de servicio? ¿Son automatizadas?		
6	¿Se monitorea, evalúa y generan reportes del proceso de administración de los niveles de servicio?		
DS2 – ADMINISTRAR LOS SERVICIOS DE TERCEROS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen políticas y procedimientos para la contratación de terceros?		
2	¿Se han asignado responsables de la supervisión de los servicios prestados por terceros?		
3	¿Las partes involucradas tienen conocimientos de los costos, etapas y expectativas del servicio?		
4	¿Los procedimientos para la contratación y control los servicios prestados por terceros se encuentran documentados?		
5	¿En el acuerdo contractual se incluye el alcance del trabajo, los servicios a suministrar, entregables, costos, cronograma, acuerdos de		

	facturación?		
6	Se han identificado los riesgos asociados a la contratación de terceros? ¿Son valorados? ¿Son evaluados y monitoreados?		
7	¿Está definida una periodicidad para la revisión del contrato y el monitoreo del cumplimiento de las condiciones operativas, legales y de control definidas en el mismo?		
DS3 – ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se realiza un proceso de planeación de la capacidad y el desempeño?		
2	¿Cuál es el nivel de satisfacción de los usuarios con respecto la capacidad del servicio actual? ¿Pueden solicitar nuevos servicios?		
3	¿Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema?		
4	¿Se hace una evaluación de la capacidad de desempeño de TI? ¿Se consideran situaciones de peor-escenario?		
5	¿Existen procesos estandarizados para enfrentar fallas por desempeño o capacidad?		
6	¿Se generan reportes con estadísticas de desempeño?		
7	¿Los planes de capacidad y desempeño están sincronizados con las proyecciones de demanda del negocio?		
DS4 – GARANTIZAR LA CONTINUIDAD DEL SERVICIO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un plan de continuidad? ¿Está documentado?		
2	¿Las pruebas de continuidad están definidas? ¿Existen responsables? ¿Existen reportes periódicos? ¿Son utilizadas en la actualización del plan de continuidad?		
3	¿El personal sigue estándares y se capacita para enfrentarse con incidentes mayores o desastres?		
4	¿Se han aplicado componentes de alta capacidad y rendimiento?		

5	¿Se implementan buenas prácticas de disponibilidad de los sistemas?		
6	¿El plan de continuidad de IT se encuentra integrado con el plan de continuidad del negocio?		
7	¿Se le realiza mantenimiento al plan de continuidad?		
DS5 – GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso de respuesta para resolver problemas de seguridad de TI? ¿Quiénes lo ejecutan?		
2	¿Es analizada la información respecto a la seguridad arrojada por los sistemas de información?		
3	¿Se han definido políticas de seguridad de la información? ¿Son aplicadas por el personal?		
4	¿Se realizan pruebas de seguridad de TI?		
5	¿Se encuentran certificados a nivel de seguridad de TI? En caso de no contar con ella ¿Están en busca de ella?		
6	¿Los usuarios están concientizados y comprometidos con las políticas de seguridad de TI? ¿Se responsabilizan de los requerimientos se seguridad de la información que manejan?		
7	¿Con qué periodicidad se evalúa la efectividad del plan de seguridad de TI?		
DS6 – IDENTIFICAR Y ASIGNAR COSTOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso de identificación y distribución de costos de TI?		
2	¿Se ha asignado un responsable de la asignación de costos?		
3	¿Existe un monitoreo y evaluación de los costos? ¿Se utiliza para optimizar los costos de recursos de TI?		
4	¿Los reportes de costos están ligados a los niveles de servicio y a los objetivos del negocio? ¿Son revisados y vigilados por los dueños de procesos de negocio?		
5	¿Existe un proceso automático de distribución de costos? ¿Se enfoca		

	en los servicios de información o en el negocio en general?		
6	¿Existe un proceso que relacione los costos de TI con los servicios prestados?		
DS7 – EDUCAR Y ENTRENAR A LOS USUARIOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La compañía cuenta con programas de entrenamiento y capacitación a los usuarios? ¿Con que periodicidad se realizan? ¿Cuál es el contenido de estos programas?		
2	¿Los procesos de entrenamiento se encuentran documentados y estandarizados?		
3	¿Los procesos de entrenamiento son monitoreados y evaluados?		
4	¿Se ha asignado un responsable del proceso de entrenamiento y capacitación?		
5	¿Los programas de entrenamiento hacen parte del plan de carrera de los empleados?		
6	¿TI es utilizada como herramienta en los procesos de entrenamiento y capacitación?		
DS8 – ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso de administración de incidentes? ¿El departamento de TI cuenta con una mesa de ayuda?		
2	¿El personal de la mesa de ayuda cuenta con herramientas que le permiten resolver los incidentes?		
3	¿Los procedimientos para la solucionar de incidentes se encuentran documentados y estandarizados?		
4	¿Existen guías de usuario y preguntas frecuentes (FAQs)? ¿Son de fácil acceso para los usuarios?		
5	¿Las consultas de usuarios, incidentes y tendencias son monitoreados y revisados?		
6	¿Se han desarrollado indicadores de desempeño para medir el		

	rendimiento de la mesa de servicio?		
DS9 – ADMINISTRAR LA CONFIGURACIÓN			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso que permita administrar la configuración de la infraestructura TI, tanto hardware como software?		
2	¿El proceso de administración de la configuración se encuentra documentado y estandarizado?		
3	¿Qué herramientas son utilizadas para la administración de la configuración? ¿Estas herramientas son similares entre plataformas o difieren en su totalidad?		
4	¿Los reportes de auditoría brindan informe esencial sobre el software y hardware con respecto a reparaciones, servicios, garantías, evaluaciones técnicas?		
5	¿Las desviaciones son monitoreadas, rastreadas y reportadas?		
6	¿Qué porcentaje de los activos de TI cubren los sistemas de administración de la configuración?		
DS10 – ADMINISTRAR LOS PROBLEMAS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen responsables para la administración de problemas?		
2	¿Existe un proceso que permita administrar problemas y resolver las causas de fondo?		
3	¿Se realizan revisiones del proceso de administración de riesgos?		
4	¿Los problemas se encuentran identificados, registrados y documentados?		
5	¿La administración de problemas está integrada con los procesos interrelacionados como la administración de incidentes, cambios, y configuración?		
6	¿El proceso de administración de problemas es proactivo y preventivo?		
7	¿Los sistemas están equipados con mecanismos automáticos de		

	advertencia y detección?		
DS11 – ADMINISTRAR LOS DATOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se ha definido responsables de la administración de los datos?		
2	¿Existen procedimientos de respaldo y recuperación de datos?		
3	¿Se encuentran definidos los propietarios o responsables de los datos?		
4	¿Se realiza algún tipo de monitoreo sobre las actividades de administración de datos (respaldo, recuperación y eliminación)?		
5	¿Los procedimientos de administración e datos esta formalizados dentro de TI?		
6	¿Qué herramientas son utilizadas en la administración de datos?		
7	¿Los requerimientos de seguridad para la administración de datos es documentada por personal clave?		
DS12 – ADMINISTRAR EL AMBIENTE FISICO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen controles ambientales contra peligros naturales y causados por el hombre? ¿Quiénes son los encargados de su implementación y monitoreo?		
2	¿Existen procedimientos para el mantenimiento de las instalaciones? ¿De quienes depende? ¿Se encuentran documentados? ¿Están estandarizados?		
3	¿La seguridad física, el mantenimiento físico y los controles ambientales tienen asignado un presupuesto?		
4	Se han definido planes de mantenimiento preventivo? ¿Con que periodicidad se realizan? ¿Se realizan horarios preestablecidos? ¿Se realizan con mayor regularidad a equipos sensibles?		
5	¿Se realiza inventario de todas las instalaciones realizadas de acuerdo con el proceso de administración de riesgos?		
6	¿El acceso de personal es monitoreado constantemente?		

7	¿Se aplican restricciones de acceso al centro de cómputo? ¿Los visitantes se registran y acompañan dependiendo del individuo o son acompañados en todo momento?		
DS13 – ADMINISTRAR LAS OPERACIONES			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Las actividades de soporte se encuentran definidas? ¿Las actividades de soporte satisfacen las necesidades de los niveles de servicio?		
2	¿Con qué frecuencia los equipos, sistemas y aplicaciones que soportan el negocio nos e encuentran disponibles?		
3	¿Se encuentran documentadas las instrucciones de qué hacer, cuándo y en qué orden?		
4	¿Los resultados de las actividades de soporte realizadas son registrados?¿Se generan reporte de los incidentes y las actividades de soporte realizadas?		
5	¿Se ha definido un responsable de las operaciones de soporte?		
6	¿Se realiza una programación de tareas? ¿Esta programación es comunicada al personal interesado?		
7	¿Con que frecuencia se reúne el personal de administración de operación con el de administración de cambios para garantizar la inclusión oportuna de cambios en producción?		
ME → MONITOREAR Y EVALUAR			
ME1 – MONITORER Y EVALUAR EL DESEMPEÑO DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La organización cuenta con un proceso de monitoreo?		
2	¿El monitoreo se encuentra implantado o se realiza cuando ocurren incidentes que ha ocasionado pérdidas a la organización?		
3	¿Se recolecta información del proceso de monitoreo para su posterior evaluación? ¿Existe un método o técnica para la recolección de información? ¿Ha sido adoptada por toda la organización?		

4	¿Las evaluaciones se realizan a nivel de procesos y proyectos individuales de TI o a nivel de los procesos en general?		
5	¿Se han definido herramientas para realizar el monitoreo de los procesos y los niveles de servicio de TI?		
6	¿Se han definido mediciones del nivel de satisfacción de los usuarios, del desempeño de TI, las estrategias y los niveles de servicio?		
7	¿Las herramientas automatizadas son utilizadas en todos los niveles de la organización para monitorear y recolectar la información de los procesos, sistemas y aplicaciones?		
ME2 – MONITORERA Y EVALUAR EL CONTROL INTERNO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La organización cuenta con procedimientos para el monitoreo del control interno?		
2	¿Se han definido responsables del monitoreo de la efectividad del control interno?		
3	¿Las evaluaciones de control interno de TI se realizan como parte de las auditorías internas tradicionales?		
4	¿Se utiliza metodologías y herramientas para realizar el monitoreo de los controles internos?		
5	¿El monitoreo de controles internos esta institucionalizado?		
6	¿Se ha definido un proceso de autoevaluaciones y revisiones de aseguramiento del control interno? ¿Quiénes son los encargados de realizar la evaluación de control interno de TI?		
7	¿Existe una base de datos de métricas para información histórica sobre el monitoreo de control interno?		
ME3 – GARANTIZAR EL CUMPLIMIENTO REGULATORIO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen procesos para mantener el cumplimiento de requisitos legales, contractuales y regulatorios? ¿Estos se siguen con regularidad o en respuesta a auditorias o revisión? ¿Han sido		

	comunicadas a todos los niveles de la organización? ¿Se encuentran actualizadas?		
2	¿Se realiza capacitación y entrenamiento sobre regulaciones y leyes externas aplicables a la organización?		
3	¿Se realiza monitoreo sobre el cumplimiento de leyes y regulaciones? ¿Existen requisitos de cumplimiento que no han sido resueltos?		
4	¿Existe contratos pro forma y procesos legales estándar para minimizar el riesgo contractual?		
ME4 – PROPORCIONAR GOBIERNO DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen procesos de planeación, entrega y supervisión de TI?		
2	¿Los procesos de gobierno de TI son monitoreados?		
3	¿Se han asignado los responsables y dueños de cada proceso?		
4	¿Los empleados impulsan los procesos de gobierno en procesos y proyectos de TI?		
5	¿Se han seleccionado procesos de TI para su mejoramiento?		
6	¿Se han implementado herramientas para el manejo y control del gobierno de TI?		
7	¿Existen indicadores de desempeño para los procesos de gobierno de TI? ¿Se encuentran registrados?		
8	¿EL personal se ha adaptado a la implementación de gobierno de TI?		

Anexo 2 LISTA DE CHEQUEO: CONOCIENDO LA INFRAESTRUCTURA DE TI

CONOCIENDO LA INFRAESTRUCTURA DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Tienen un esquema de la infraestructura tecnología?		
2	¿Cuántas personas conforman el área de TI?		
3	¿Qué tipo de vínculo laboral tienen con la empresa?		
4	¿Cuáles son los servicios que ofrece el área de TI en la organización?		
5	¿Existe un inventario de equipos?		
6	¿Existe un inventario de software? ¿ el software esta licenciado?		
7	¿Qué aplicaciones se encuentran instaladas en los servidores, cuales son desarrollados en la organización y cuales con terceros?		
8	¿Qué tipo de soporte reciben las aplicaciones y qué tipo de licencias se tiene de estas?		
9	¿Cómo está organizada lógicamente la red de la organización?		
10	¿Las aplicaciones tienen control de acceso, los sistemas operativos tienen control de acceso?		
11	¿Existen logs de ingresos de usuarios a los sistemas operativos de servidores, aplicativos y equipos, dominios?		

12	¿Están protegidos los logs?
13	¿Existen controles para la base de datos se usan claves compartidas?
14	¿Se realizan acciones en las tablas de la base de datos por fuera de los aplicativos? ¿Existe un procedimiento para hacerlo? ¿Están protegidas las tablas críticas?
15	¿El personal de soporte tiene full control de los aplicativos? Quien autoriza Existen procedimientos para autorizarlo.
16	¿Están protegidos archivos carpetas que contienen información relevante?
18	¿Están documentados la configuración de los equipos de red, servidores?
19	¿Están registrados los incidentes de fallas en los aplicativos y/o servicios; existen bitácoras de los mismos?
20	¿Están documentados y autorizados los procedimientos de cambios de parámetros de software?
21	¿La configuración de los equipos activos de red y servidores tiene en cuenta configuraciones seguras ideales, se realizan análisis de vulnerabilidades?

INFRAESTRUCTURA	SI	NO	NA
1. ¿Están definidas las áreas de los servidores?			
2. ¿La ubicación de los servidores se encuentra lejos de las interferencias electromagnéticas?			

3. ¿La temperatura del área de servidores está en el rango permitido?			
4. ¿Existen ventanas y puertas del cuarto de servidores que dan al exterior de la empresa?			
5. En caso de existir ventanas y puertas ¿éstas son fáciles de abrir?			
6. ¿El cuarto de servidores está cerca a una vía principal?			
7. ¿Se presentan vibraciones en el piso de los servidores?			
8. ¿Existen extintores en el área de servidores?			
9. ¿Los armarios y/o rack están protegidos?			
10. ¿El cableado de red esta ordenado y etiquetado? Existe un plano.			
11. ¿Existen sistemas de detección de incendios? Pólizas de seguros, números de emergencia bomberos.			
12. ¿Existen sistemas de detección de incendios?			
13. Existen pisos falsos, cámaras de seguridad, registro de accesos autorizados al área de centro de dato?			
14. ¿Existen UPS para soportar la carga eléctrica de los servidores?			
15. ¿Se le hace mantenimiento a las UPS?			
16. ¿Se cuenta con planta eléctrica cuando el fluido de red pública falle?			
17. ¿Se le realiza mantenimiento preventivo a la planta eléctrica, quien lo realiza.			

18. ¿se verifica cantidad de combustible de la planta eléctrica y de reserva?			
19. ¿El estado de los tableros de distribución eléctrica es adecuado?,			
20. ¿Se realizan mediciones periódicas de voltaje de red pública y planta eléctrica y se lleva registro de ellas?			
21. ¿Existe transferencia automática? Se hacen pruebas?			
22. ¿Se tiene un registro del mantenimiento realizado a los servidores?			
23. ¿Los procedimientos de mantenimiento de servidores se encuentran documentados?			
24. ¿Se hace mantenimiento a los equipos de cómputo?			
25. ¿Los procedimientos de mantenimiento de equipos de cómputo se encuentran documentados?			
26. ¿Se tiene un registro de las modificaciones y/ó actualizaciones realizadas a los equipos?			
27. ¿Se tiene una copia exacta de los sistemas operativos para apoyo en caso de pérdida ó daños?			
28. ¿Se cuenta con un directorio actualizado de todo el personal de trabajo?			

ACCESO	**SI**	**NO**
¿Existe un sistema de control de acceso del personal a las instalaciones de la empresa?		
¿Los empleados están totalmente identificados como empleados de la empresa?		

¿Existen restricciones de horario para el acceso a las instalaciones de la empresa?		
¿Existen controles de acceso a personas ajenas a la empresa?		
¿Existen controles de registro de equipos portátiles ajenos a la empresa?		
¿Existe un control de registro de los equipos que salen de la empresa?		
¿Existe un sistema de control de acceso a los servidores?		
¿Se hace un registro de los accesos concedidos y denegados?		
¿Los procedimientos de acceso están documentados?		
¿Los cargos de manejo de llaves de las oficinas están identificados?		
¿Existe un CCTV en la empresa?		

SEGURIDAD DE LA INFORMACION		
¿Se cuenta con un inventario por áreas de los medios magnéticos?	**SI**	**NO**
¿Cada uno de los medios magnéticos cuenta con una etiqueta de identificación?		
¿Externamente se lleva un registro de qué contiene cada medio magnético?		
¿Existe un procedimiento que diga cómo etiquetar los medios magnéticos?		
¿Existe un registro de los medios magnéticos con su respectivo responsable?		
¿Existen políticas de manejo (préstamo y acceso) de los medios magnéticos?		
¿Existe un procedimiento establecido para la destrucción de los medios magnéticos?		
¿Existe un registro de la destrucción de los medios magnéticos?		
¿Se realizan backups de seguridad de la información?		

En caso de realizar backups de seguridad de la información, ¿se tiene establecida la periodicidad?		
¿Los procedimientos de backups de la información se encuentran documentados?		
¿Los backups se encuentran almacenados un lugar con acceso restringido?		
¿El lugar de almacenamiento de backups es adecuado?		
¿Se realizan pruebas de la funcionalidad de los backups?		
¿los backup están protegidos (encriptados)?		
¿Los procedimientos de actualización de equipos se encuentran documentados?		
¿Se tiene un inventario actualizado de licencias?		
¿Existen políticas de actualización de licencias?		
¿Existen políticas establecidas de actualización de antivirus?		
¿Existen políticas establecidas para instalación de parches en los equipos?		
¿Existen políticas establecidas para la creación de contraseñas?		
¿Existen políticas establecidas de control de acceso lógico?		
¿Existen políticas establecidas para el acceso remoto?		
¿Existen políticas establecidas para el manejo del correo electrónico?		
POLITICAS		
¿Existen políticas establecidas para la contratación con terceras partes?		
¿El procedimiento de contratación con terceras partes se encuentra documentado?		
¿Se firman contratos de confidencialidad cuando existen contratos con terceros?		

ANEXO 3 LISTADO FOTOGRÁFICO

RACK

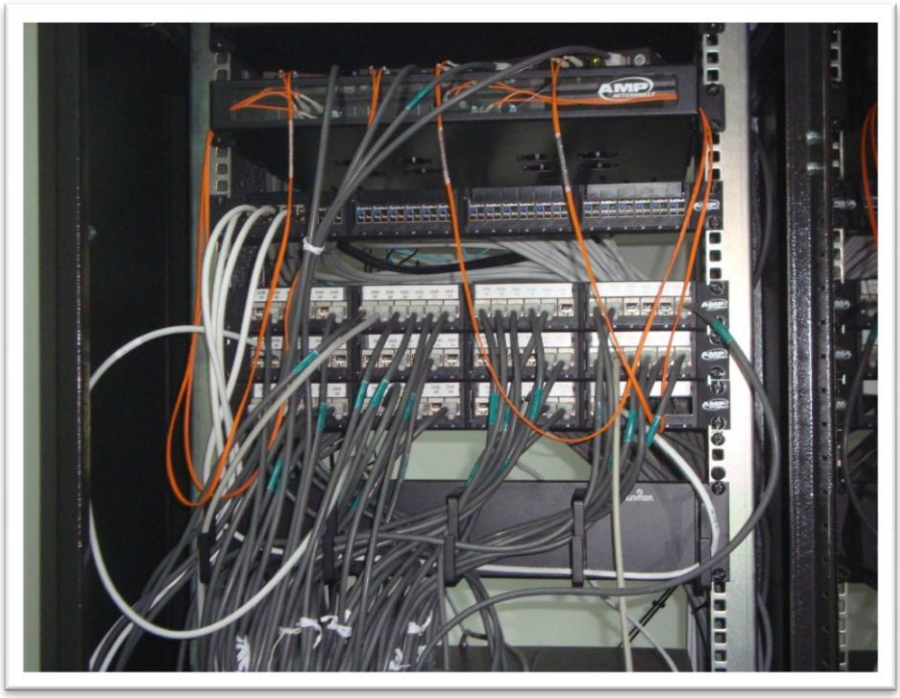
Control biométrico de acceso al centro de datos (data center)

Guarda de seguridad área administrativa y acceso a sala de sistemas

Extintores especializado para centro de datos

Tablero de control automático de incendio

Gabinete de aire acondicionado para centro de datos

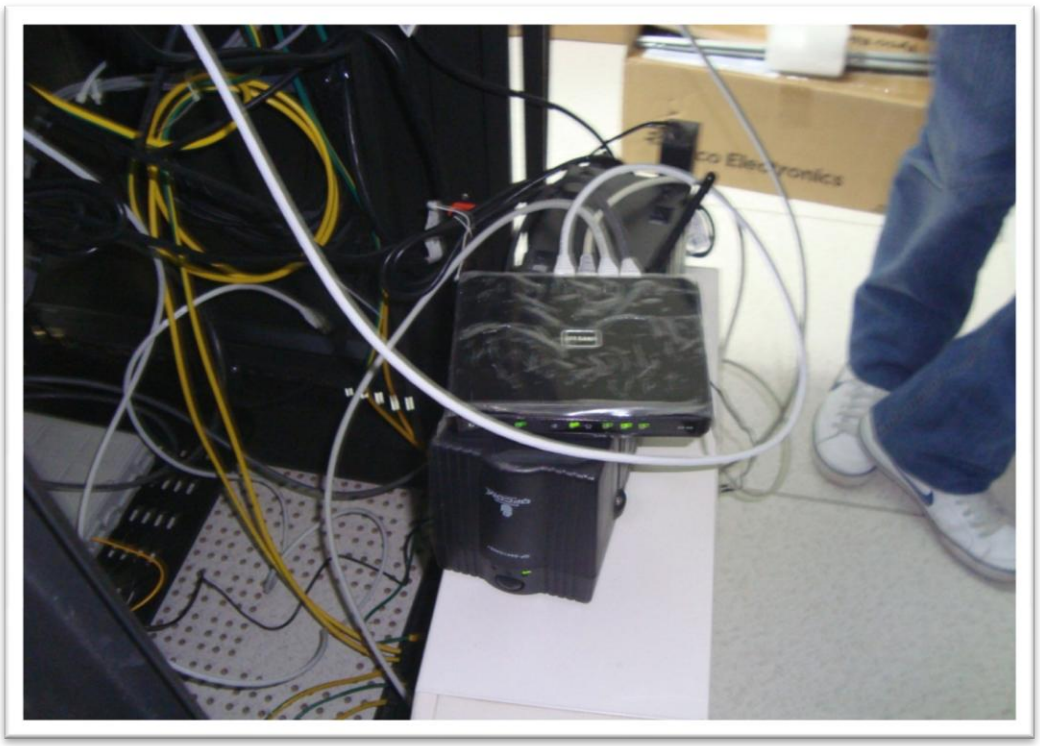


Tablero de Distribución Eléctrica

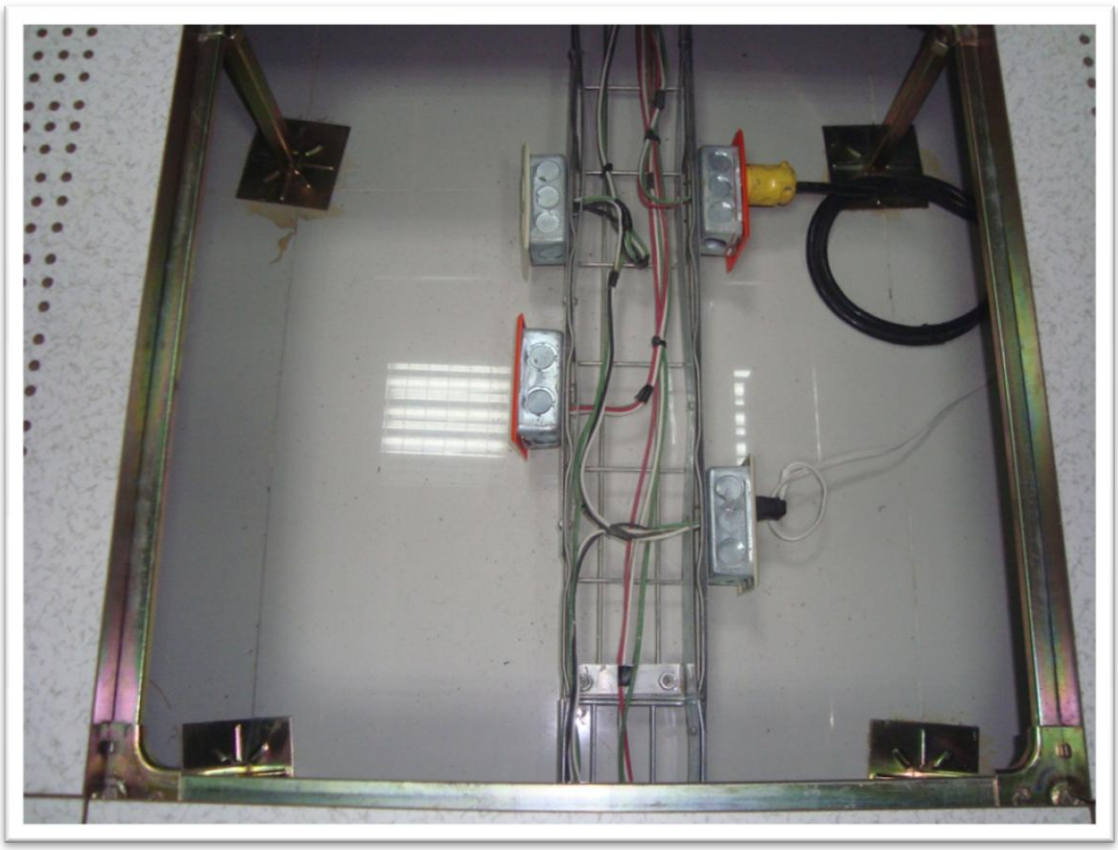
Tomas Eléctrico Regulado y Tomas de Red

Objetos Inflamables en el Centro de Datos

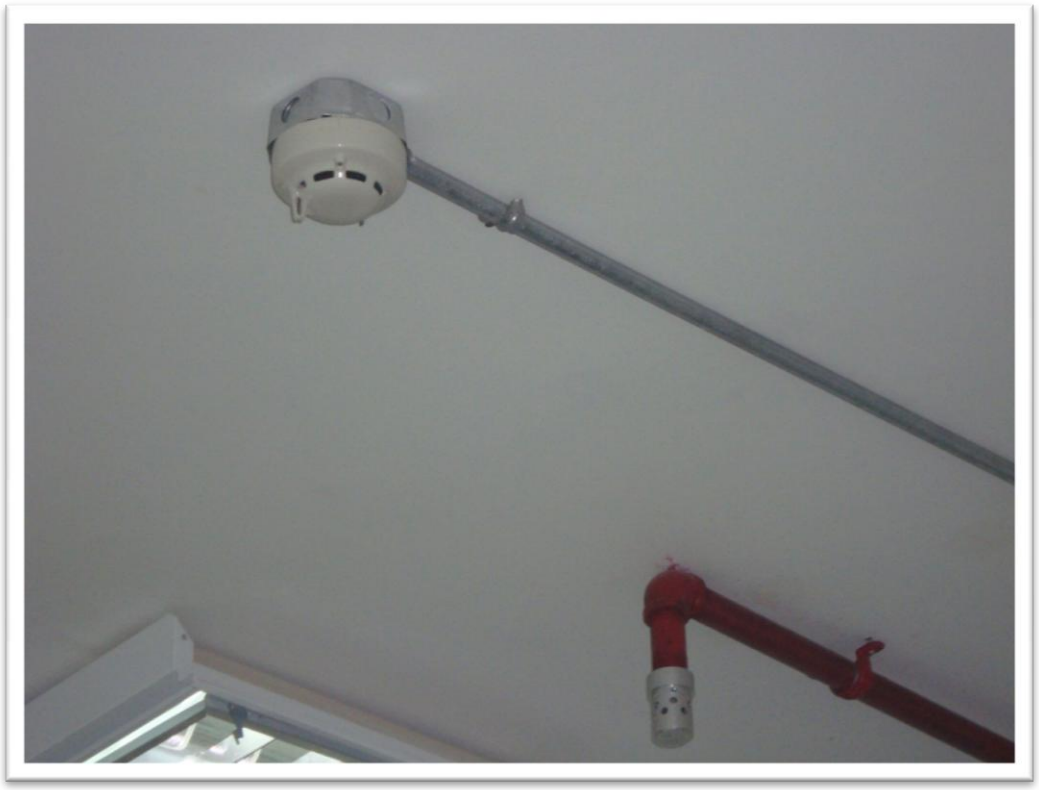
Mala Organización de Equipos en Gabinetes en el Centro de Datos



Piso Falso de Centro de Datos



Detector de Incendio en el Centro de Datos



Monitoreo de Cámaras Centro de Datos

Estructura de Cableado

Centro de Sistemas

ANEXO 1

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Fecha: 25 de enero de 2012

Marque con una X

Tesis [X] **Trabajo de Grado** [ ]

Yo **Norberto Castaño Urbina** identificado con C.C No 19.705.464 actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado **DISEÑO DEL PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR** presentado y aprobado en el año 2012 como requisito para optar al título de **Especialización En Auditoria De Sistemas**; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 25 días del mes de Enero de 2012

EL AUTOR - ESTUDIANTE. Norberto Castaño Urbina

FIRMA

ANEXO 1

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Fecha: 25 de enero de 2012

Marque con una X

Tesis [X] **Trabajo de Grado** [ ]

Yo **Cristian Raúl Fuentes Castillo**, identificado con C.C. No. 77.097.103 actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado **DISEÑO DEL PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR** presentado y aprobado en el año 2012 como requisito para optar al título de **Especialización En Auditoria De Sistemas**; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 25 días del mes de Enero de 2012

EL AUTOR - ESTUDIANTE. Cristian Raúl Fuentes Castillo

FIRMA

ANEXO 2
FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO: **DISEÑO DEL PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR**

SUBTÍTULO, SI LO TIENE:

_____

_____

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Fuentes castillo Castaño Urbina	Cristian Raúl Norberto

DIRECTOR (ES)

Apellidos Completos	Nombres Completos
Ardila Montaño Díaz	Víctor Manuel Roberto Carlos

JURADO (S)

Apellidos Completos	Nombres Completos

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos
Ardila Montaño	Víctor Manuel

TRABAJO PARA OPTAR AL TÍTULO DE: ESPECIALISTA EN AUDITORIAS DE SISTEMAS DE INFORMACIÓN

FACULTAD: CONTADURÍA PUBLICA

PROGRAMA: Pregrado ____ Especialización X

NOMBRE DEL PROGRAMA ESPECIALIZACIÓN EN AUDITORIAS DE SISTEMAS DE INFORMACIÓN

CIUDAD: Barranquilla **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO: 2012**

NÚMERO DE PÁGINAS: 156

TIPO DE ILUSTRACIONES:

- ☐ Ilustraciones
- ☐ Láminas
- ☐ Retratos
- [x] Tablas, gráficos y diagramas
- ☐ Planos
- ☐ Mapas
- [x] Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica):

Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ___ Beta Max ___ ¾ ___ Beta Cam ____ Mini DV ____ DVD Cam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cuál ? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

_____

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Unidad de Procesos Técnicos de la Unidad de información en el correo biblioteca@cuc.edu.co, donde se les orientará).*

ESPAÑOL	**INGLÉS**
GOBIERNO DE TI	IT GOVERNANCE

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS:(Máximo 250 palabras-1530 caracteres):

El presente proyecto se denomina DISEÑO DEL PLAN ESTRATEGICO DE TECNOLOGIA INFORMATICA Y MODELO DE GESTION DE SERVICIOS DE TECNOLOGIA DE INFORMACION (TI) PARA LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLEDUPAR fue realizado conceptualmente en cuatro estándares para la construcción de un modelo de Gobierno de TI y que gozan de gran aceptación mundial, por lo que han sido denominados como “Mejores Prácticas”.

El Modelo Cobit, las normas ISO 27001, 27002, 20000 e ITIL representan las mejores prácticas, para su implementación en las organizaciones y la articulación de cada una de ellas conforman un modelo guía útil para una adecuada planificación de TI, para las entidades de salud como la ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ – VALLDUPAR brindara una oportunidad de alinear las estrategias de TI con las estrategias del hospital, de alcanzar el uso optimo de todos sus recursos que ayudaran a satisfacer las necesidades de la entidad y los requisitos de los usuarios, Cumplir con la legislación, prestar un mejor servicio, revisarse y mejorarse de forma continua. Con la implementación de estos estándares contribuirá a proporcionar una base de control de TI en las entidades de salud.

SUMMARY

This project is called the PLAN strategy of technology INFORMATICS and model of management of services of technology of information (TI) for LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ - VALLEDUPAR was conceptually done in four standards for the construction of a model of it governance and which enjoyed great worldwide acceptance, by what have been referred to as "Best practice". .

The Model Cobit, ISO 27001, 27002, 20000 and ITIL represents best practice for implementation in organizations and the articulation of each of them make a model useful guide for proper planning of IT for health organizations that LA ESE HOSPITAL ROSARIO PUMAREJO DE LOPEZ - VALLEDUPAR would provide an opportunity to align TI strategies with the strategies of the hospital, to achieve the optimum use of all resources that help meet the needs of the entity and the user requirements, comply with legislation, providing a better service, reviewed and improved continuously. With the implementation of these standards will help to provide a basis for control of TI in health agencies..